Version: 2011-04-05

RCCMD – Multiple Server Shutdown Software

Benutzerhandbuch

Version: 2011-04-05

Urheberrechts-Erklärung zum geistigen Eigentum und Umgang mit vertraulichen Informationen

Die Informationen in diesem Benutzerhandbuch sind nicht bedingte Anweisungen und können ohne Ankündigung verändert werden. Obwohl GENEREX versucht hat, präzise Informationen in diesem Dokument bereitzustellen, übernimmt GENEREX keine Verantwortung für die Genauigkeit dieser Informationen.

GENEREX ist nicht verantwortlich für jeden indirekten, speziellen, daraus folgenden oder unbeabsichtigten Schaden, ohne Einschränkungen, verlorener Gewinne oder Einkommen, Kosten von Austausch Gütern, Verlust oder Beschädigung von Daten, die sich durch den Gebrauch dieses Dokumentes oder das hier beschriebenen Produkt ergeben.

GENEREX als Hersteller der genannten Produkte, übernimmt keine Verpflichtungen mit diesen Informationen. Die Produkte, die in diesem Handbuch beschrieben werden, wurden auf der alleinigen Basis von Informationen für Geschäftspartner gegeben, damit diese ein besseres Verständnis für die GENEREX Produkte erhalten.

GENEREX erlaubt seinen Geschäftspartnern die Informationen, die in diesem Dokument enthalten sind, an Dritte weiterzugeben, ebenso an das Personal in deren Firma oder ihren eigenen Kunden, elektronisch, manuell, in Form von Fotokopien oder Ähnlichem. GENEREX gibt an, dass der Inhalt nicht verändert oder angepasst werden darf, ohne schriftliche Genehmigung von GENEREX.

Alle Rechte, Titel und Interessen am GENEREX Markenzeichen BACS oder Firmenzeichen (registriert oder nicht registriert) oder der Geschäftswert bzw. das geistige Eigentum von GENEREX, das Urheberrecht und die Produkt-Patente sind exklusiv und ohne Einschränkungen im Eigentum von GENEREX.

GENEREX wird jede Beanstandung über den Inhalt dieses Dokumentes zeitnah abwickeln. Kommentare oder Beanstandungen zu diesem Dokument sollten an die GENEREX Systems Vertriebsgesellschaft mbH adressiert werden.

Das Urheberrecht der Europäischen Union ist gültig (Copyright EU).

Copyright (c) 1995-2011 GENEREX GmbH, Hamburg, Deutschland.

Alle Rechte vorbehalten.

Revision	History	Date
-001	Erstausgabe	10/2008
-011	Update: Funktion “Senden einer Nachricht an alle RCCMD Clients”	10/2008
-012	Added: RCCMD auf XEN und ESX Server	12/2008
-013	RCCMD mit SSL	12/2008
-014	Update: UNIX multiple Sender Konfiguration	01/2009
-015	Added: Alternative SSL Konfiguration	02/2009
-016	Added: Syntax Schalten der Outputs	03/2009
-017	Added: RCCMD Relay auf UNIX	03/2009
-018	Update: Installation von RCCMD	06/2009
-019	Update: RCCMD Installation mit InstallAnywhere	07/2009
-020	Added: Silent Installation Windows	08/2009
-021	Added: Grafische RCCMD Relay Konfiguration Windows	08/2009
-022	Added: Kombi-Silent- und Konfigurations Installation	10/2009
-023	Added: RCCMD auf ESXi 4.0.x	10/2009
-024	Added: Silent Installation UNIX	11/2009
-025	Added: Console Installation UNIX	11/2009
-026	Added: Know How Pool	11/2009
-027	Added: Automatisches Zurücksetzen des Redundanz Alarms	01/2010
-028	Added: Grafische RCCMD Relay Konfiguration UNIX/MAC	03/2010
-029	Added: Configuration on Windows 2008 Server Core x64	07/2010
-030	Added: RCCMD FAQ	08/2010
-031	Added: RCCMD on ESXi 4.1 with vMA 4.1	11/2010

Inhalt

1. Was ist die RCCMD Software? 5
2. Netzwerk Shutdown mit RCCMD 5
3. Installation / Konfiguration von RCCMD für Windows 7
3.1 Installation von RCCMD 7
3.1.1 Silent Installation für die RCCMD Installation 18
3.1.2 RCCMD Silent Installation mit Übernahme eigener Konfiguration 19
3.2 Testen des Shutdown.Bat Files 19
3.3 Alte Installation von RCCMD 21
3.4 Einstellungen der Berechtigung für den RCCMD Dienst 23
3.5 Installation von RCCMD mit Redundanz (ab RCCMD V3) 28
3.5.1 Automatisches Zurücksetzen des Redundanz Alarms 30
3.6 Der RCCMD Client als Relay Station 32
3.7 RCCMD auf Windows 95/98 35
3.8 RCCMD auf Windows NT/2000/XP/2003/2008 36
3.9 RCCMD auf Windows 2008 Server Core x64 37
3.10 RCCMD mit SSL auf Windows 38
3.10.1 RCCMD mit eigenen SSL Zertifikaten 45
3.11 Testen der RCCMD Verbindung 46
3.11.1 Testen der RCCMD 2 Verbindung 46
4. RCCMD auf NovellNetWare 48
5. RCCMD auf UNIX (mit grafischer Oberfläche) 52
5.1 RCCMD mit Redundanz (ab RCCMD V3) 61
5.2 Silent Installation für die RCCMD Installation 63
5.3 Console Installation für die RCCMD Installation 64
5.4 UNIX RCCMD Konfiguration mit CURSES Library 67
5.5 Der RCCMD Client als Relay Station 80
5.6 RCCMD mit SSL auf UNIX 82
5.6.1 RCCMD mit eigenen SSL Zertifikaten 86
6. RCCMD auf DEC VMS 87
7. RCCMD auf MAC OS 9 90
8. RCCMD auf MAC OS 10.X 94
9. RCCMD auf Citrix XEN Server 101
10. RCCMD auf VMware 103
10.1 RCCMD auf VMware ESX 104
10.2 RCCMD auf VMWARE ESXi 105
11. RCCMD AS400-Client 115
12. RCCMD FAQ 115
Appendix 117
A OpenSSL 117
B Syntax zum Schalten von Ausgängen 117
C Know How Pool 118
D Abbildungen 118

1. Was ist die RCCMD Software?

RCCMD ist eine Netzwerk Client Software, die das Empfangen von Shutdowns und Nachrichten von USV Servern wie UPSMAN UPS Software, CS121 SNMP Adapter oder jeder anderen RCCMD kompatiblen Netzwerkkarte von anderen, lizensierten Partnern ermöglicht.

RCCMD ist die erfolgreichste *Multiple Server Shutdown Software* und *Nachrichten Tool* in der gesamten USV Welt.

2. Netzwerk Shutdown mit RCCMD

Das Programm RCCMD wurde entwickelt, um Befehle auf einem Remote System in einem TCP/IP Netzwerk auszuführen. RCCMD arbeitet wie das RSH (Remote Shell), das man aus der UNIX Umgebung kennt. Innerhalb der UPS Management Software wird RCCMD zum Herunterfahren von mehren Servern benutzt, die alle von einer einzelnen USV versorgt werden. Für diese Aktion wurde einer dieser Server als *UPS Master Server* konfiguriert.

Installieren Sie die UPS Management Software *UPSMAN* auf ihrem UPS Master Server und verbinden Sie ihn mit der USV. Alternativ können Sie einen CS121 SNMP Adapter verwenden. Die anderen Server sind nur mit der USV Stromversorgung verbunden, da keine RS232 Verbindung notwendig ist. Installieren Sie RCCMD auf diesen Remote Maschinen, und erstellen Sie eine Shutdown-Routine für jedes System. Diese Shutdown-Routine könnte ein Batch File, ein Shell Script oder NFC File sein, das die Befehle für dieses Sytem beinhaltet. Danach fügen Sie RCCMD zu der Shutdown-Aktion oder der Event Konfiguration des UPS Master Servers hinzu.

Nun haben Sie eine Workstation in ihrem Server Netzwerk, die die USV überwacht. Die anderen Server führen RCCMD aus und erwarten das RCCMD Signal von dem USV Master Server. Im Falle eines Stromausfalls würde der Master ein Shutdown-Signal für das Server Netzwerk wie folgt veranlassen. Die Shutdown-Aktion des USV Master Servers würde RCCMD starten und ein entsprechendes Signal an alle Server in der Liste senden. RCCMD würde den programmierten Befehl auf den Empfängern ausführen.

Bitte beachten Sie, dass es erforderlich ist, RCCMD in 2 verschiedenen Funktionen zu installieren:

1. Als Sender auf dem USV Master Server

   (RCCMD –s) (send)

2. Als Empfänger (Hintergrund Prozess) auf den Empfangs-Servern

   (RCCMD –l) (listen)

Im Gegensatz zu RSH, enthält RCCMD nicht den auszuführenden Befehl, der versendet wird, aber dafür setzt es den Befehl im Empfangs-Prozess ab. Dies bietet einen entscheidenden Sicherheitsvorteil im Gegensatz zu RSH. Darüber hinaus überprüft der

Empfänger dabei, welche Workstation das RCCMD Signal sendet und entscheidet, ob der auszuführende Befehl akzeptiert wird oder nicht.

Achtung: **Wir empfehlen immer mit der IP Adresse einen Netzwerk Shutdown via RCCMD durchzuführen und nicht den Hostnamen zu verwenden.**

RCCMD Version 2 oder höher

Die erweiterte Version von RCCMD ist in der Lage, Befehle auf Remote Systemen, ein Shutdown Batch File in dem TCP/IP Port 6003, ein Email-Batch, Log File Einträge usw. auszuführen. Der RCCMD 2 Sender (UPSMAN oder CS121 SNMP Adapter) sendet ein entsprechendes RCCMD Signal, und der RCCMD 2 Client startet das entsprechende Batch File.

Der initiierte Befehl wird immer vom UPSMAN oder dem CS121 gesendet, welcher auf dem RCCMD Client ausgeführt wird.

Beispiel: Der CS121 soll eine NET SEND (Netzwerknachricht) in ein Windows NT Netzwerk senden. Der Adapter kann so konfiguriert werden, dass er während eines Stromausfalls eine RCCMD Message gesendet wird, die individuell vom Benutzer verfasst werden kann.

Beim Empfangen der Nachricht startet der RCCMD 2 Client ein Batch File und sendet die NET SEND Message. Initiator ist hierbei der UPSMAN oder der CS121. Dadurch ist es möglich, Nachrichten oder Emails in unterschiedliche Netzwerke mit verschiedenen Betriebssystemen zu senden, initiiert durch einen USV Alarm.

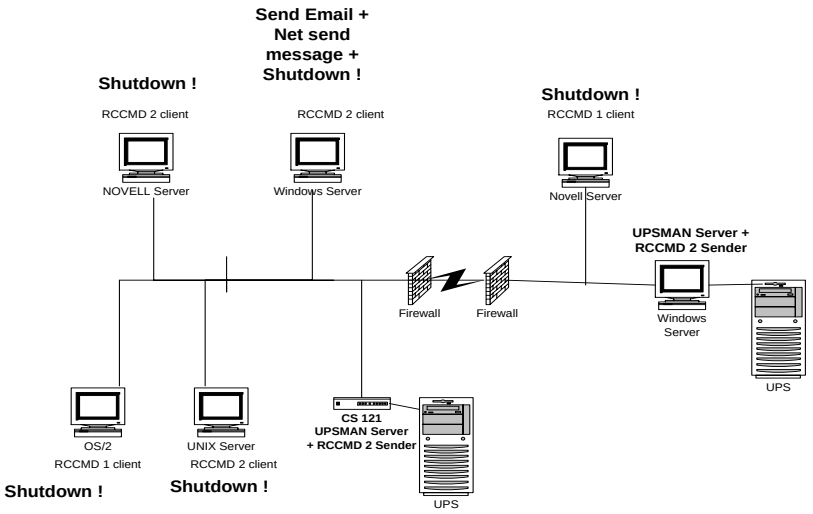


Abb. 1: RCCMD und UPSMAN in einer Netzwerkumgebung

3. Installation / Konfiguration von RCCMD für Windows

3.1 Installation von RCCMD

Bevor Sie mit der Installation beginnen, sollten Sie sich vergewissern, dass Sie über volle Administrator Rechte verfügen.

Step 1:	Legen Sie die CD in das Laufwerk ihres Computers, oder laden Sie die Software in ein Verzeichnis ihrer Wahl herunter.
Step 2:	Führen Sie die “Setup.exe” aus, kopieren Sie die Daten auf ihre Festplatte, und wählen Sie die gewünschte Sprache aus.
Step 3:	Tragen Sie den Lizenzschlüssel in das Feld ein und wählen Sie das entsprechende Betriebssystem aus. Die Lizenz ermittelt, für welches Modul die Installation geeignet ist.

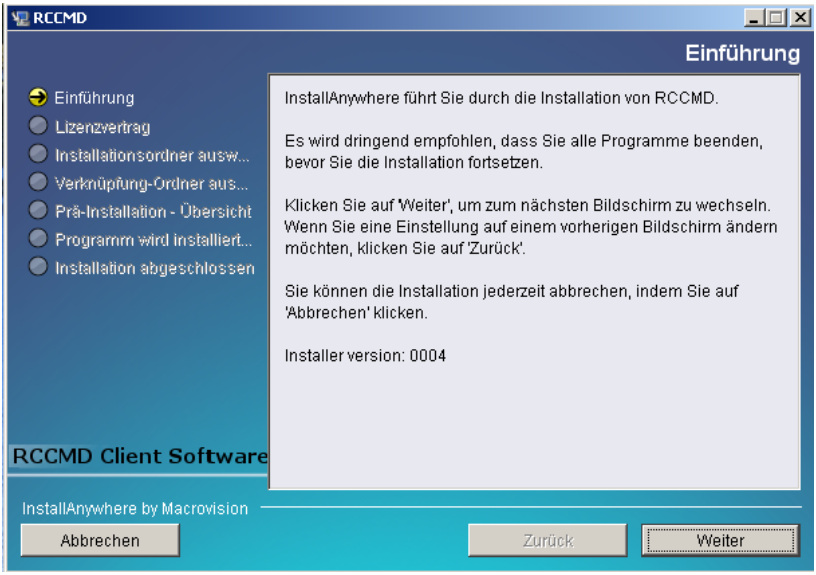

RCCMD
Einführung
Einführung
Lizenzvertrag
Installationsordner ausw...
Verknüpfung-Ordner aus...
Prä-Installation - Übersicht
Programm wird installiert...
Installation abgeschlossen
InstallAnywhere führt Sie durch die Installation von RCCMD.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die Installation fortsetzen.
Klicken Sie auf 'Weiter', um zum nächsten Bildschirm zu wechseln. Wenn Sie eine Einstellung auf einem vorherigen Bildschirm ändern möchten, klicken Sie auf 'Zurück'.
Sie können die Installation jederzeit abbrechen, indem Sie auf 'Abbrechen' klicken.
Installer version: 0004
RCCMD Client Software
InstallAnywhere by Macrovision
Abbrechen
Zurück
Weiter

Abb. 2: Einführung

In dem Menü auf der linken Seite des Fensters, können Sie den Fortschritt der Installation erkennen. Klicken Sie auf “Weiter”, um fortzufahren.

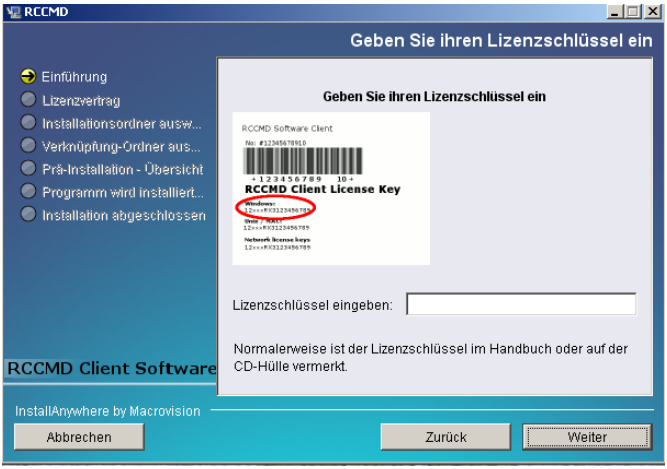


Abb. 3: Lizenzschlüssel Eintrag

Geben Sie hier Ihre Lizenznummer ein, ein Bild mit rotem Rahmen zeigt ein Beispiel. Klicken Sie auf “Next”, um fortzufahren.

Achtung:

Wird an dieser Stelle eine falsche Lizenznummer eingegeben, ist die RCCMD ClientSoftware auf eine 30 Tage Trial-Version eingestellt. Bitte informieren Sie sich bei Ihrem USV Händler nach der vollständigen Lizenz, falls diese nicht der Original CD beilag.

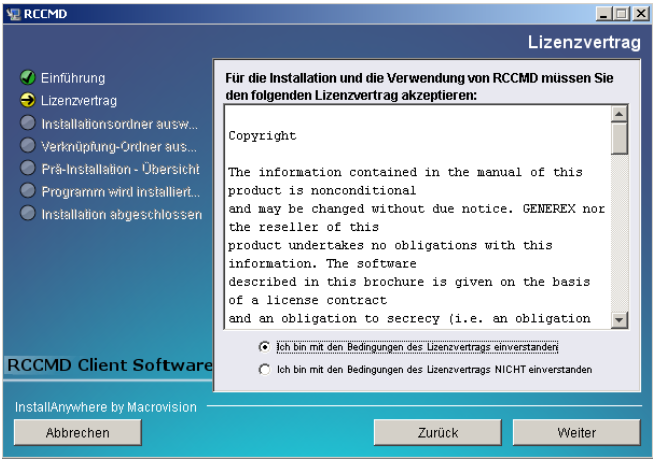

RCCMD
Lizenzvertrag
Einführung
Lizenzvertrag
Installationsordner ausw...
Verknüpfung-Ordner aus...
Prä-Installation - Übersicht
Programm wird installiert...
Installation abgeschlossen
Für die Installation und die Verwendung von RCCMD müssen Sie den folgenden Lizenzvertrag akzeptieren:
Copyright
The information contained in the manual of this product is nonconditional and may be changed without due notice. GENEREX nor the reseller of this product undertakes no obligations with this information. The software described in this brochure is given on the basis of a license contract and an obligation to secrecy (i.e. an obligation
Ich bin mit den Bedingungen des Lizenzvertrags einverstanden
Ich bin mit den Bedingungen des Lizenzvertrags NICHT einverstanden
RCCMD Client Software
InstallAnywhere by Macrovision
Abbrechen
Zurück
Weiter

Abb. 4: Lizenzvertrag

Lesen und bestätigen Sie den Lizenzvertrag, und klicken sie auf “Weiter”.

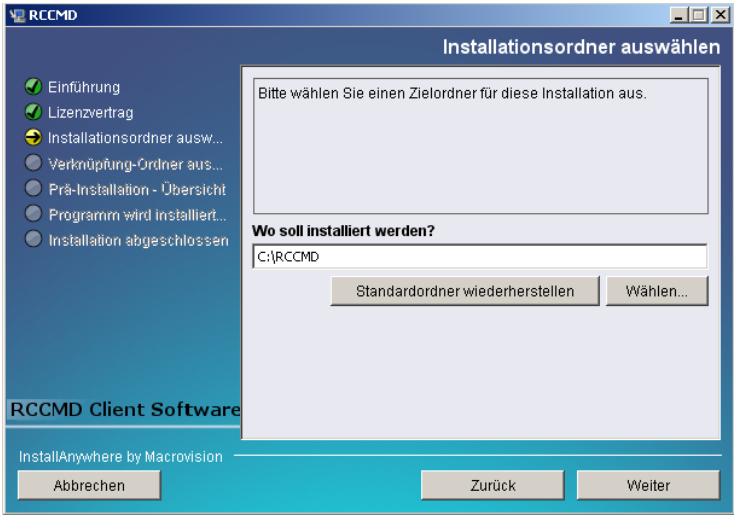


Abb. 5: Auswahl Installationsordner

Geben Sie den Pfad an, in dem Sie die Software installieren möchten. Standard ist das Verzeichnis “RCCMD” auf der Festplatte “C:”.

Attention:

Wenn Sie ein Programm oder Batchfile mit RCCMD ausführen möchten, ist es erforderlich, dass dieses Programm oder Batchfile im Installationsverzeichnis \RCCMD (*nicht* in Program Files\RCCMD wie Standard) liegt oder auf dem Verzeichnis ein Suchpfad gesetzt ist.

In dem nächsten Menü können Sie eine neue Programmgruppe erstellen, deren Bestimmungsort festlegen oder eine Verknüpfung auf dem Desktop erstellen.

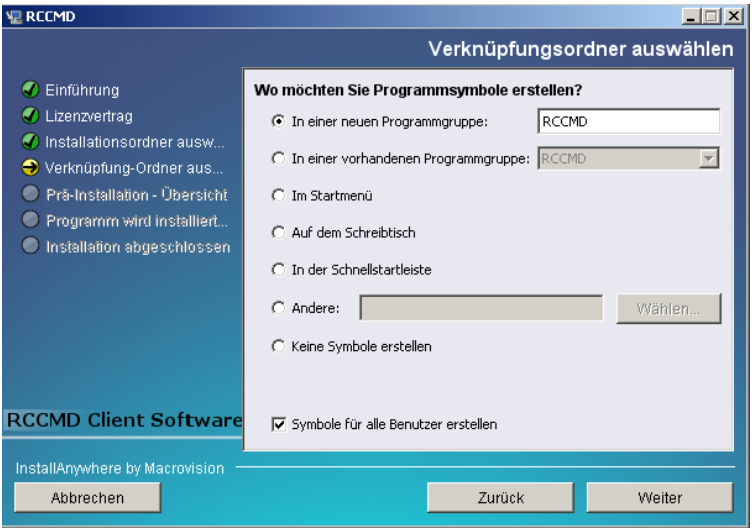


Abb. 6: Auswahl Verknüpfungsordner

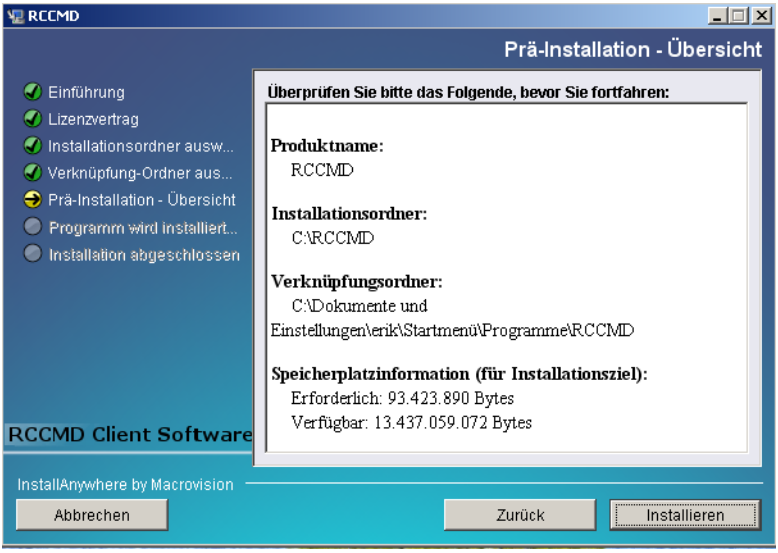


Abb. 7: Preinstallations Übersicht

Klicken Sie auf “Installieren”, um fortzufahren.

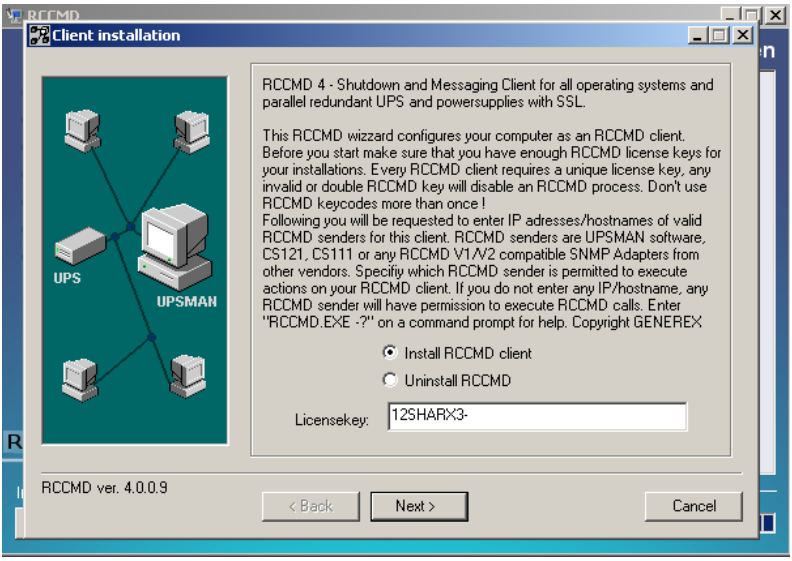

Client installation
UPS
UPSMAN
RCCMD 4 - Shutdown and Messaging Client for all operating systems and parallel redundant UPS and powersupplies with SSL.
This RCCMD wizzard configures your computer as an RCCMD client. Before you start make sure that you have enough RCCMD license keys for your installations. Every RCCMD client requires a unique license key, any invalid or double RCCMD key will disable an RCCMD process. Don't use RCCMD keycodes more than once !
Following you will be requested to enter IP adresses/hostnames of valid RCCMD senders for this client. RCCMD senders are UPSMAN software, CS121, CS111 or any RCCMD V1/V2 compatible SNMP Adapters from other vendors. Specifiy which RCCMD sender is permitted to execute actions on your RCCMD client. If you do not enter any IP/hostname, any RCCMD sender will have permission to execute RCCMD calls. Enter "RCCMD.EXE -?" on a command prompt for help. Copyright GENEREX
Install RCCMD client
Uninstall RCCMD
Licensekey:
12SHARX3-
RCCMD ver. 4.0.0.9
< Back
Next >
Cancel

Abb. 8: Client Installation

Klicken Sie auf “Next”.

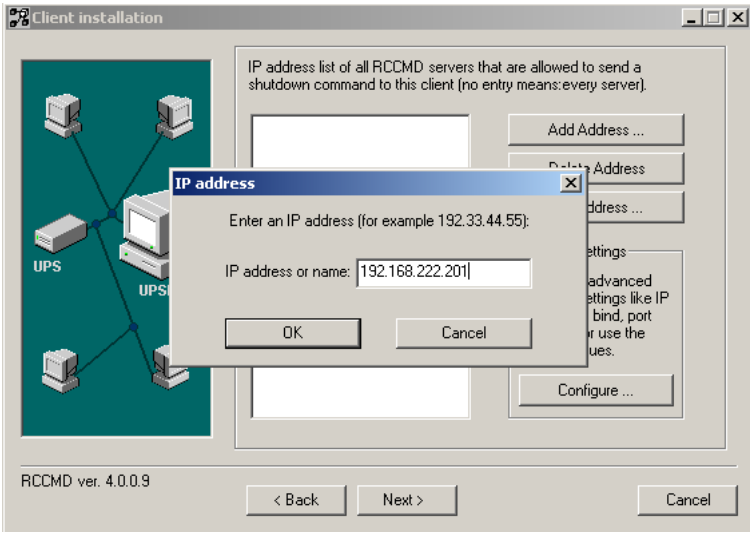


Abb. 9: Eingabe IP-Adresse

Step 4: Tragen Sie die IP-Adresse des RCCMD Servers ein, der authorisiert ist, ein Shutdown Signal zu senden.

Attention:

Wenn Sie hier keine Adresse eintragen, ist jeder Server in der Lage, einen Shutdown an diesen Client zu senden. Wenn mehr als ein CS121 oder UPSMAN in dem Netzwerk existieren, befinden Sie sich in der Redundanz Situation. Hier müssen mehrere Adressen als authorisierte Sender eingetragen werden.

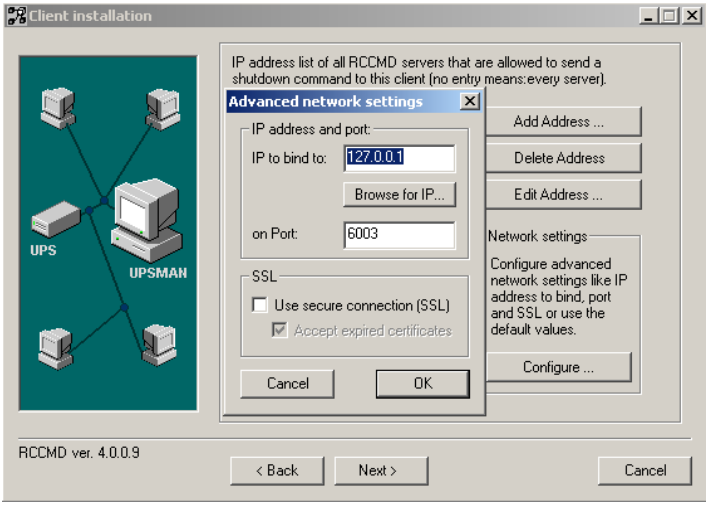


Abb. 10: Erweiterte Netzwerk Einstellungen

Step 5:

Wenn Sie eine SSL Verbindung nutzen möchten, klicken Sie auf “Configure…” und haken Sie die “SSL-Box” an.

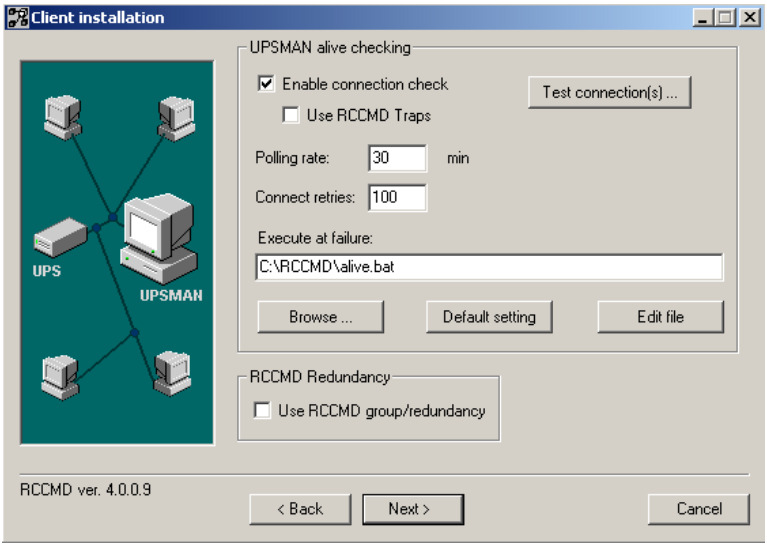


Abb. 11: UPSMAN Alive Checking / Redundanz Fenster

Step 6:

Wenn Sie die Funktion “UPSMAN Alive Checking” nutzen möchten (empfohlen), haken Sie die entsprechende Box an. Dieser Check ist ein Signal, das an den CS121 oder UPSMAN via Port 5679 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “Alive.Bat” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt. Die Polling Rate (Standard 30 Minuten) definiert den Interval der UPSMAN Abfrage, connect retries (Verbindungswiederholungen, Standard 5) bedeutet, das nach 5 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

Die Funktion “Use RCCMD Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigen. Wenn aktiviert, wird diese Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Wenn Sie auf “Test connections…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5679 wird getestet).

Wenn Sie auf “Browse…” klicken, werden Sie eine Auswahl der Standard Batch Files erhalten.

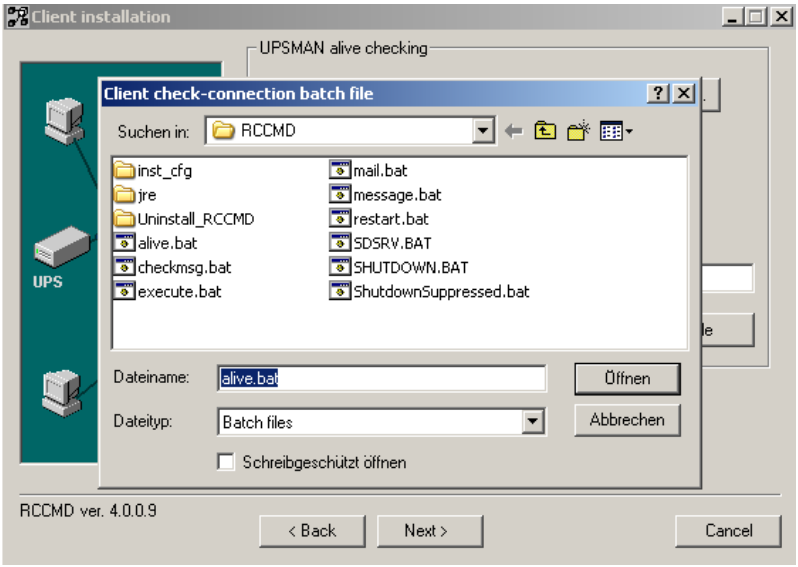


Abb. 12: Client Check Connection Batch File Fenster

Wenn Sie auf „Default Setting“ klicken, werden Sie zurück zum Alive.Bat File gelangen.

Bei einem Fehler von dem UPSMAN Alive Check können Sie eine auszuführende Datei konfigurieren oder das Standard File “Alive.Bat” editieren:

@echo off

rem * "messagetext" %1 == ip-address, %2 == date, %3 == time *** "title" -c counter for beeps**

start /b msg.exe "Check Upsman %1 failed (%2, %3)" "ATTENTION RCCMD:" -c:1

Klicken Sie auf “Next”.

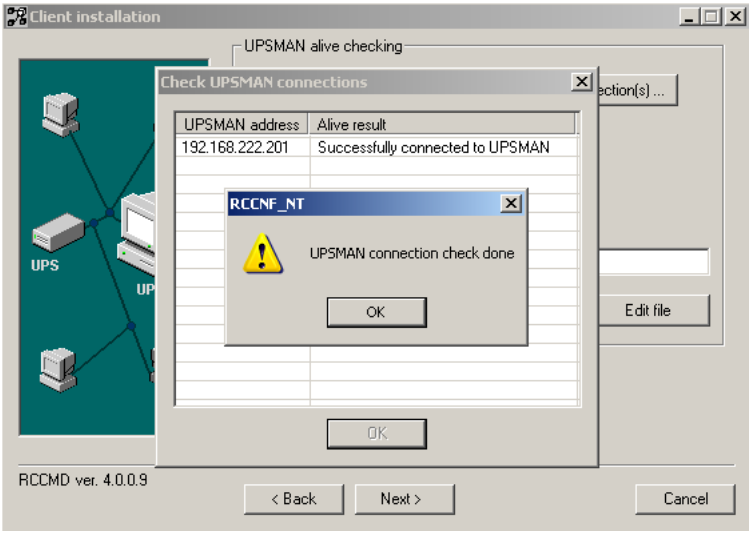


Abb. 13: Check UPSMAN Connections Fenster

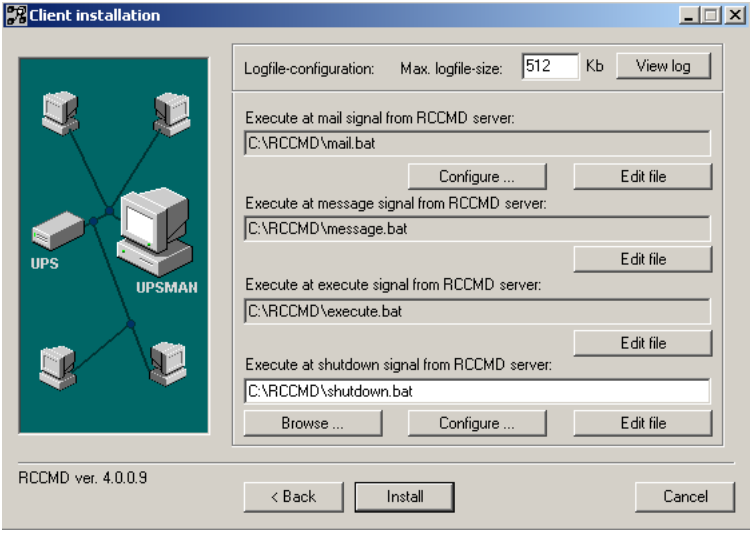


Abb. 14: Konfiguration der Batch Files Fenster

Step 6: Sie können die Log File Grösse konfigurieren und die auszuführenden Bat Files editieren.

rccmd.log - Editor

Datei Bearbeiten Format Ansicht ?

```
09/10/2008,03:10:17, RCCMD: UPSMAN/RCCMD Evaluation version - testing purpose only, this software will stop working in 30 days.
09/10/2008,03:10:17, RCCMD: RcvThreadUdp started
09/10/2008,03:10:17, RCCMD: RCCMD Listen Mode started.
09/10/2008,08:46:37, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,08:52:33, RCCMD: Broadcast-Message from 192.168.202.92 received
09/10/2008,09:08:15, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,10:15:24, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,13:26:54, RCCMD: RcvThreadUdp stopped
09/10/2008,13:26:54, RCCMD: RCCMD Listen Mode stopped
09/10/2008,13:27:01, RCCMD: RcvThreadUdp started
09/10/2008,13:27:01, RCCMD: SendThreadCheckUpsman started
09/10/2008,13:27:01, RCCMD: RCCMD Listen Mode started.
09/10/2008,13:27:01, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:01, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:01, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:28, RCCMD: RcvThreadUdp stopped
09/10/2008,13:27:28, RCCMD: RCCMD Listen Mode stopped
09/10/2008,13:27:28, RCCMD: SendThreadCheckUpsman stopped
09/10/2008,13:27:32, RCCMD: SendThreadCheckUpsman started
09/10/2008,13:27:32, RCCMD: RcvThreadUdp started
09/10/2008,13:27:32, RCCMD: RCCMD Listen Mode started.
09/10/2008,13:27:32, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:32, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:32, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,16:05:05, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,16:38:32, RCCMD: RcvThreadUdp stopped
09/10/2008,16:38:33, RCCMD: RCCMD Listen Mode stopped
09/10/2008,16:38:33, RCCMD: SendThreadCheckUpsman stopped
09/10/2008,16:38:38, RCCMD: SendThreadCheckUpsman started
09/10/2008,16:38:38, RCCMD: RcvThreadUdp started
09/10/2008,16:38:38, RCCMD: RCCMD Listen Mode started.
```

Abb. 15: RCCMD Log File

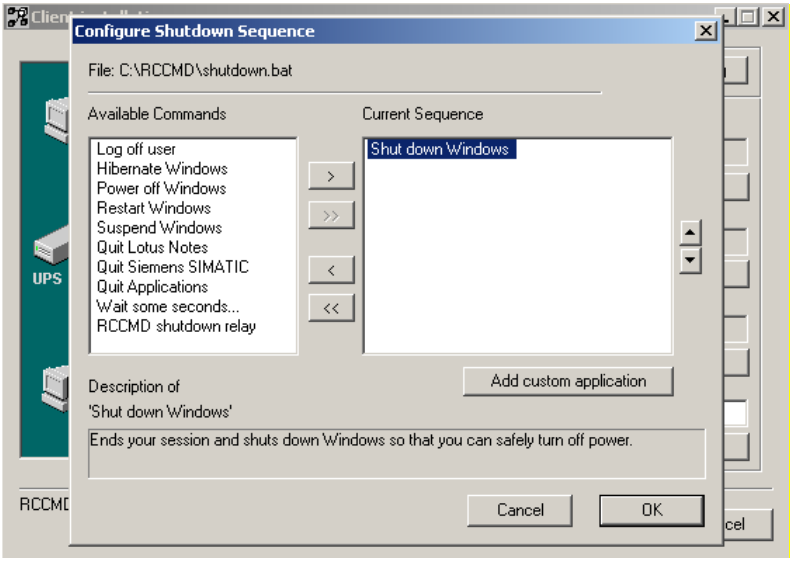


Abb. 16: RCCMD Shutdown Sequenz Konfiguration

Die folgenden Befehle sind für die Shutdown Sequenz Konfiguration erhältlich:

Achtung: **Die Shutdown Sequenz wird von oben nach unten "abgearbeitet", d.h. der "Shutdown Windows" –Befehl sollte ganz unten in der**

Reihenfolge stehen, da danach natürlich keine weiteren Befehle mehr ausgeführt werden können.

Log Off user: Beendet Ihre Sitzung, verlassen der Workstation, die im Betrieb bleibt.

Hibernate Windows: Ist der Ruhestand, bei dem der Inhalt des Arbeitsspeichers auf die Festplatte geschrieben wird.

Power off Windows: Beendet Ihre Sitzung, fährt Windows herunter und wird stromlos.

Restart Windows: Beendet Ihre Sitzung, fährt Windows herunter und startet es neu.

Suspend Windows: Ist der Ruhezustand, bei dem der Inhalt des Arbeitspeichers NICHT auf die Festplatte geschrieben wird.

Quit Lotus Notes: Schliesst Lotus Notes vor dem Herunterfahren von Windows. Bitte konfigurieren Sie eine Verzögerung nach diesem Befehl.

Quit Siemens SIMATIC: Schliesst die WIN CC Datenbank vor dem Herunterfahren von Windows. Bitte konfigurieren Sie eine Verzögerung nach diesem Befehl.

Quit applications: Schliesst alle Anwendungen vor dem Herunterfahren von Windows.

Wait some seconds: Wartet eine Weile in Sekunden, bis der nächste Befehl ausgeführt wird.

RCCMD shutdown relay: Leitet einen RCCMD Shutdown Befehl an eine andere Workstation weiter.

Shutdown Windows: Beendet Ihre Sitzung und fährt Windows herunter, sodass Sie sicher die Stromzufuhr unterbrechen können.

Die Standard Shutdown.Bat beinhaltet Folgendes:

rem created by setup

@echo off

set path=C:\WINDOWS\;C:\WINDOWS\system32\;C:\Program Files\RCCMD

ExitWin.exe shutdown force

@cls

3.1.1 Silent Installation für die RCCMD Installation

In der RCCMD Software besteht die Möglichkeit, eine Silent Installation (Hintergrundinstallation) zu aktivieren. Bevor man diese Funktion nutzen möchte, sind Einstellungen in der Datei „installer.properties“ notwendig. Diese befindet sich auf der UPS Management CD im Verzeichnis \Rccmd\Windows\12.

```
## This file provides Values to alter the behaviour of the installer.
## You can preset Values for some internal Variables.
## For the installer to find and use this file it is necessary to either rename
##  this file or pass a parameter to the installer when calling it.
##
## If this file is called 'installer.properties' or has the same name as the
##  installer, e.g. 'install_RCCMD.properties' then the installer should
##  automatically use this file.
##
## To call the installer with a parameter providing a properties file, the
##  installer need the parameter '-f' in this case the command line call looks
##  somewhat like this: "install_RCCMD.exe -f silent-installer.properties".
##
## To set the installer User Interface without providing the variable in the
##  properties file, the parameter '-i' can be used.
##  E.g. "install_RCCMD.exe -i silent"
##  The interface options are "silent,gui,console" the gui option is default.

## This will set the User Interface of the installer
#INSTALLER_UI=silent

## This presets the Licensekey. This value is necessary for a silent
##  installation, because there is no other way to pass this information to
##  the installer.
#GXLICENSEKEY=

## The Dialogbutton variable contains the answer to the pop-up questions whether
##  the RCCMD should be started at system boot and wether it should be started now.
##  the value '0' resembles the answer 'Yes' the value '1' (default) corresponds
##  to 'no'.
#CHOSEN_DIALOG_BUTTON=0

## Select the language for the installed version of RCCMD by setting the
##  INST_LANG variable to the desired country-code
##  (e.g.: el,en,es,de,fr,he,it,ja,ko,pt,ru,tr,zh_cn).
#INST_LANG=en
```

Abb. 17: Dateiinhalt „installer.properties“

Um die Silent Installation zu aktivieren, müssen Sie das Doppelkreuz vor der Variabel `INSTALLER_UI=silent` entfernen. Zusätzlich ist die Eingabe eines Lizenzschlüssels hinter der Variabel `GXLICENSEKEY=` erforderlich. Wenn Sie die RCCMD Software nicht in das Standardverzeichnis `C:\Program Files\RCCMD` installieren möchten, beachten Sie bei der Eingabe des Installationspfades, dass das Backslash-Zeichen ein Backslash-Zeichen und ein Leerzeichen im Pfad ebenfalls ein Backslash-Zeichen benötigen, z. B.:

```
USER_INSTALL_DIR=C:\\program\ files\\RCCMD
```

Mit der Variabel `CHOSEN_DIALOG_BUTTON=0`können Sie die Antwort auf die Frage definieren, ob der UPSMAN Dienst nach dem Systemstart automatisch gestartet werden soll. „0“ bedeutet ja, „1“ bedeutet nein.

Die Sprachauswahl können Sie mit der Variabel INST_LANG=de treffen, damit Ihnen bei der Konfiguration von der RCCMD Software die Tooltipps in der gewünschten Sprache zur Verfügung stehen.

3.1.2 RCCMD Silent Installation mit Übernahme eigener Konfiguration

Nach dem Sie die Datei „installer.properties“ ensprechend bearbeitet haben, ist es möglich, eine eigene RCCMD Konfiguration zu erstellen und „silent“ zu installieren. Dazu ist es erforderlich, die RCCMD Konfiguration einmal manuell durchzuführen via normal SETUP über den RCCMD Wizard.

Danach kann diese Konfiguration aus der Registry wie folgt in eine Datei exportiert werden:

- Klicken Sie mit der rechten Maustaste in dem Verzeichnis HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\rccmd\ auf „Parameters“, wählen „Export“ aus, und speichern Sie die Datei als „WIN95/NT4 Registration File mit dem Namen „rccmd.reg“.

- Legen Sie die Datei „rccmd.reg“ in das Verzeichnis ab, in dem sich das RCCMD-Installer-Paket befindet.

- Öffnen Sie die Datei „rccmd.reg“ mit einem Editor, und löschen Sie die komplette Zeile, die den Lizenzschlüssel enthält.

- Erstellen Sie mit einem Editor eine neue Windows-Batch-Datei (* .bat), zum Beispiel mit dem Namen „InstallAndConfigRCCMD.bat“, deren Inhalt wie folgt ausehen sollte:

```
@echo off
cls
echo *** Installation of RCCMD, please wait... ***
installRCCMD.exe
echo *** Importing RCCMD configuration file ***
regedit.exe -s rccmd.reg
echo Ready
```

Nun können Sie eine kombinierte RCCMD Silent Installation und Konfiguration starten, in dem Sie die soeben erstellte Windows-Batch-Datei „InstallAndConfigRCCMD.bat“ ausführen.

3.2 Testen des Shutdown.Bat Files

Wir empfehlen Ihnen, das editierte Shutdown.Bat File zu testen. Das Shutdown Programm EXITWIN.EXE ist vordefiniert. Für die Syntax-Hilfe zu diesem Shutdown Tool, tippen Sie einfach RCCMD -? in dem RCCMD Verzeichnis. Sie können aber auch ein eigenes Shutdown Tool verwenden, das mit dieser Software kompatibel ist.

Achtung:

Wenn Ihre Konfiguration einwandfrei im Debug Modus läuft, bedeutet dies nicht gleichzeitig, dass es auch einwandfrei als RCCMD Windows NT Dienst funktioniert. Bitte vergewissern Sie sich, dass der RCCMD Dienst mit administrativer Berechtigung gestartet wurde, denn sonst könnte es passieren, dass nur uneingeschränkte Programme (z.B. notepad.exe) ausgeführt werden, aber keine Shutdowns (häufigste Fehlermeldung: "Adjust Token Privileges failed").

Die komplette Befehls-Syntax für die NT-Konsole für RCCMD im Lauscher-Modus:

rccmd [–debug] -l [-a IP adress] [–h hostname] [-p port] "command"

Der Befehl kann ein Programm oder ein anderes Batch File auf dieser Workstation ausführen. Der Befehl sollte mit voller Pfadangabe eingegeben werden. Die "-p" Port Option kann eingefügt werden, wenn Sie RCCMD mehrmals auf einer Workstation ausführen möchten, um mehrere Befehle ausführen zu lassen. Der Standard Port ist 6003, benutzen Sie andere, freie Ports, um verschiedene Befehle auszuführen.

RCCMD in dem Sender Modus:

rccmd [–debug] -s [-a IP adress] [-h hostname] [-p port]

Dieser Befehl wird regelmässig in dem Batch File von dem Sender genutzt (shutdown.bat) und sendet ein Echosignal (ping) an die IP-Adresse der Workstation oder deren Hostnamen. Wenn das Echo beantwortet wurde, könnte der nächste Befehl ausgeführt werden (RCCMD –s) etc.

Wenn Sie die Editierung der Batch Files abgeschlossen haben, klicken Sie auf "Install".

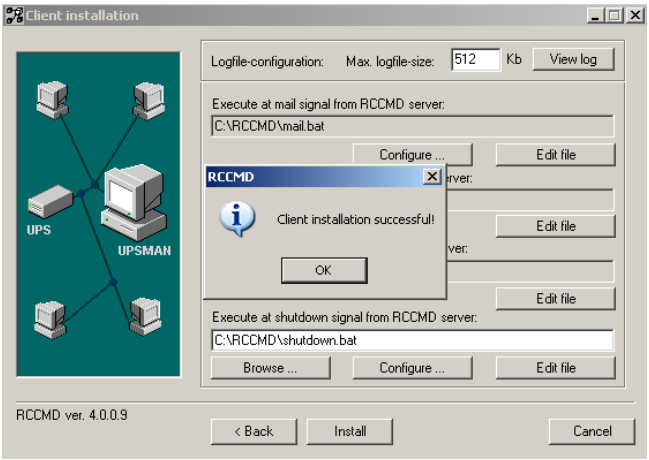


Abb. 18: Erfolgreiches Client Installations Fenster

RCCMD läuft nun als Dienst mit automatischen Start. Um den automatischen Start zu konfigurieren, nutzen Sie die administrative Berechtigung, die Systemsteuerung und verändern Sie dort die Einstellungen in den Diensten.

WICHTIG: RCCMD als Dienst mit lokaler Desktop Interaktion ist in der Lage, lokale Shutdowns auszuführen. Um spezielle Aktionen via RCCMD durchzuführen, z.B. Starten einer NETSEND Nachricht oder andere Befehle, benötigt RCCMD extra Berechtigungen! Diese Berechtigungen werden in der Systemsteuerung/Dienste konfiguriert.

Senden einer Nachricht an alle RCCMD Clients

Um eine Nachricht an alle RCCMD Clients senden zu können, nutzen Sie bitte folgende Syntax:

rccmd –se "MSG_TEXT ups_says_hello_world" –a 192.9.200.255

Der RCCMD Client, der die Nachricht erhalten soll, muss entweder die IP-Adresse des Senders in seiner IP-Adressen-Liste eingetragen haben, oder die Liste muss leer sein. Da der CS121 nicht fähig ist, UDP-Broadcasts zu senden, muss man im RCCMD Client die o.g. Syntax eintragen, sodass der Client als Relay-Station die Nachricht weiterleitet. Von einem Windows-, UNIX- oder MAC OS-RCCMD Sender ist es kein Problem, diese Nachricht zu senden.

3.3 Alte Installation von RCCMD

Bevor Sie mit der Installation beginnen, sollten Sie sich vergewissern, dass Sie über volle Administrator Rechte verfügen.

Step 1:	Legen Sie die CD in das Laufwerk ihres Computers, oder laden Sie die Software in ein Verzeichnis ihrer Wahl herunter.
Step 2:	Führen Sie die "Setup.exe" aus, kopieren Sie die Daten auf ihre Festplatte, und wählen Sie die gewünschte Sprache aus.
Step 3:	Tragen Sie den Lizenzschlüssel in das Feld ein und wählen Sie das entsprechende Betriebssystem aus. Die Lizenz ermittelt, für welches Modul die Installation geeignet ist.

Achtung:

Wenn Sie hier eine falsche Lizenznummer eingeben, wird RCCMD automatisch als 30-Tage-Testversion installiert. Bitte wenden Sie sich an ihren USV Händler für eine korrekte Lizenz.

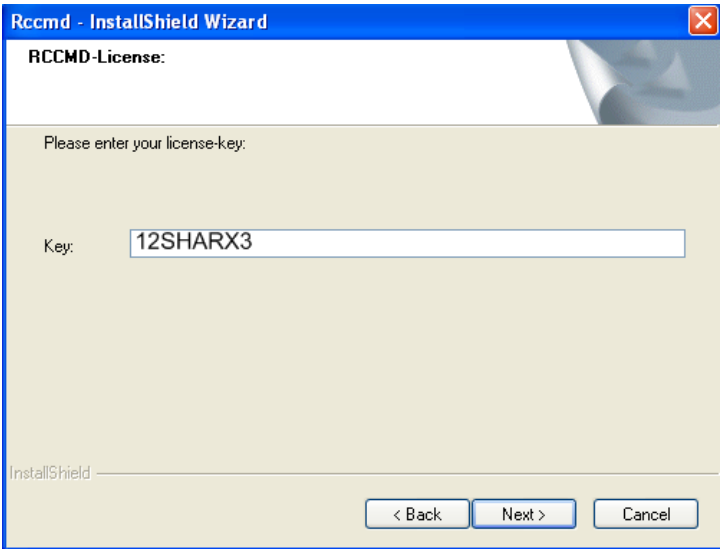


Abb. 19: Lizenzschlüssel Eintrag

Sie benötigen einen speziellen Lizenzschlüssel für die RCCMD Software. Sie können den Schlüssel mit dem “RX3” in dem ersten Teil der Lizenz erkennen. Dieser Schlüssel muss separat bestellt werden.

Wählen Sie den Setup Typ aus. “Complete” bedeutet, dass alle Features installiert werden. “Custom” ist nur für fortgeschrittene Benutzer.

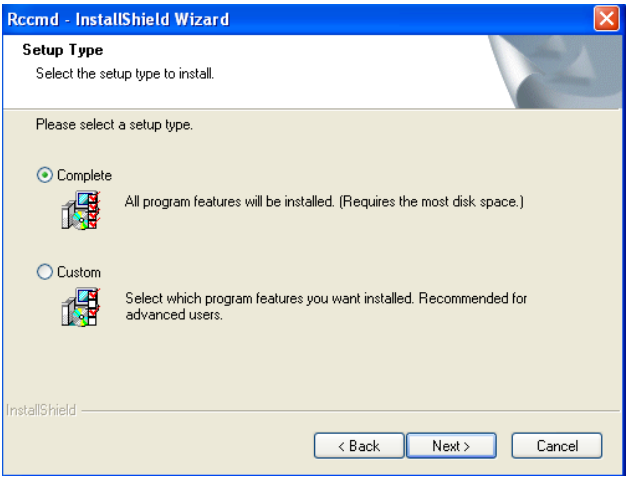

Rccmd - InstallShield Wizard
Setup Type
Select the setup type to install.
Please select a setup type.
Complete
All program features will be installed. (Requires the most disk space.)
Custom
Select which program features you want installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

Abb. 20: RCCMD Setup Typ Fenster

Nach dem Sie die Geschäftsbedingungen akzeptiert haben und den “Install Wizard” beendeten, werden Sie das “Client Installations Fenster” sehen.

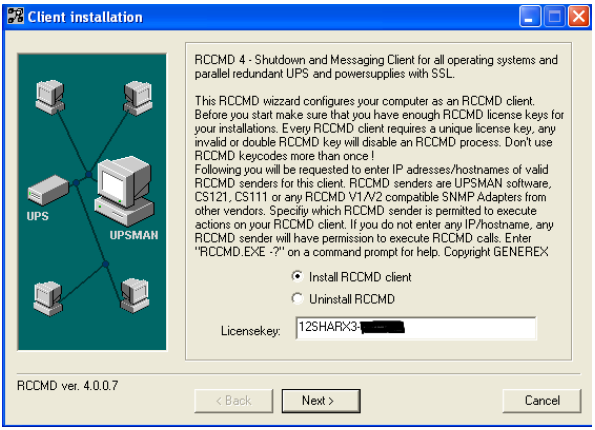

Client installation
UPS
UPSMAN
RCCMD 4 - Shutdown and Messaging Client for all operating systems and parallel redundant UPS and powersupplies with SSL.
This RCCMD wizzard configures your computer as an RCCMD client. Before you start make sure that you have enough RCCMD license keys for your installations. Every RCCMD client requires a unique license key, any invalid or double RCCMD key will disable an RCCMD process. Don't use RCCMD keycodes more than once !
Following you will be requested to enter IP adresses/hostnames of valid RCCMD senders for this client. RCCMD senders are UPSMAN software, CS121, CS111 or any RCCMD V1/V2 compatible SNMP Adapters from other vendors. Specifiy which RCCMD sender is permitted to execute actions on your RCCMD client. If you do not enter any IP/hostname, any RCCMD sender will have permission to execute RCCMD calls. Enter "RCCMD.EXE -?" on a command prompt for help. Copyright GENEREX
Install RCCMD client
Uninstall RCCMD
Licensekey:
12SHARX3-
RCCMD ver. 4.0.0.7
< Back
Next >
Cancel

Abb. 21: Eingabe Lizenzschlüssel

Für die weitere Konfiguration schauen Sie bitte auf die Seite 11, Step 4 in diesem Handbuch.

3.4 Einstellungen der Berechtigung für den RCCMD Dienst

Öffnen Sie das Eigenschaften-Menü für den RCCMD Dienst (via Systemsteuerung, Verwaltung, Dienste).

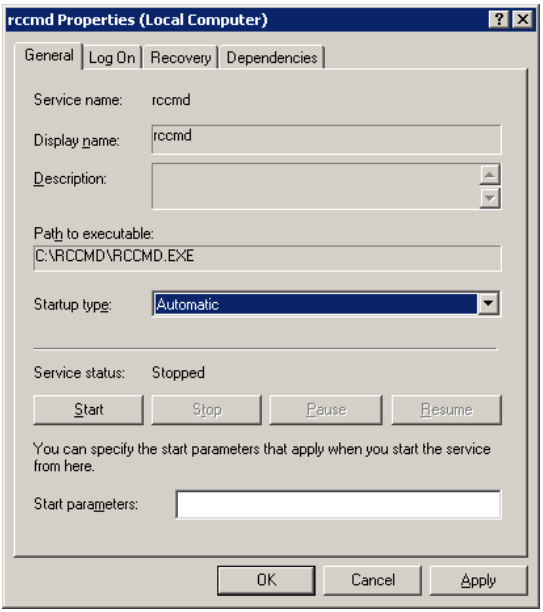


Abb. 22: RCCMD Eigenschaften Fenster

Klicken Sie auf den Kartenreiter “Log On”.

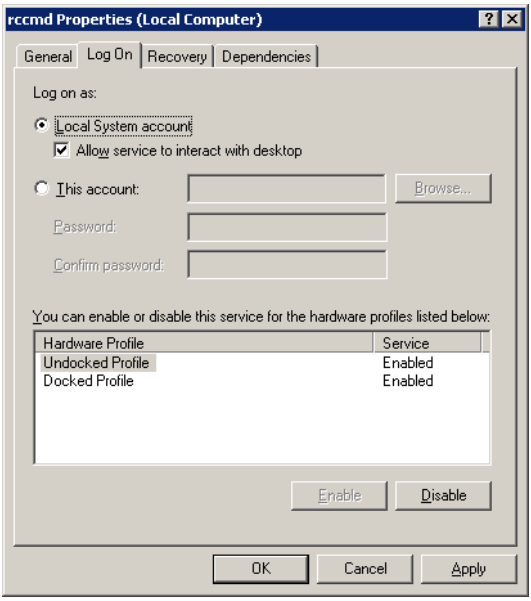


Abb. 23: RCCMD Eigenschaften Log On Fenster

Klicken Sie in den Kreis “Local System account”, **lösche**n **Sie die Passwörter** ,und klicken Sie auf “Browse…”.

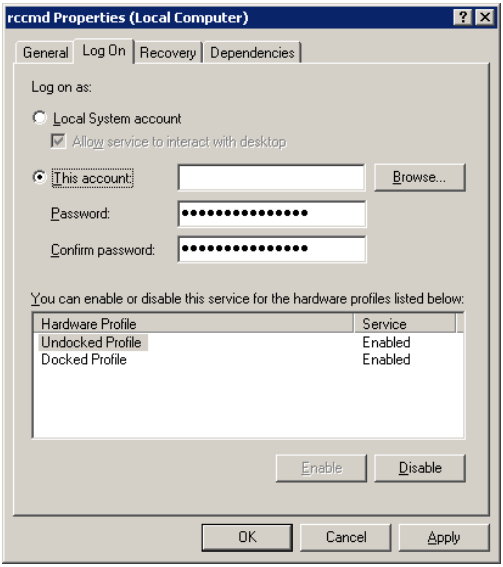


Abb. 24: RCCMD Eigenschaften Passwort-Bestätigung

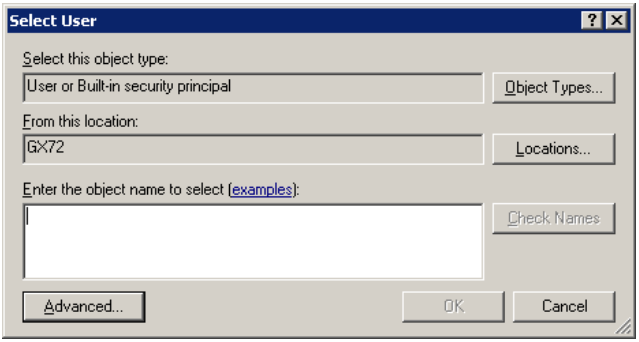


Abb. 25: Select User Fenster

Klicken Sie auf “examples”, um einen Objektnamen auszuwählen.

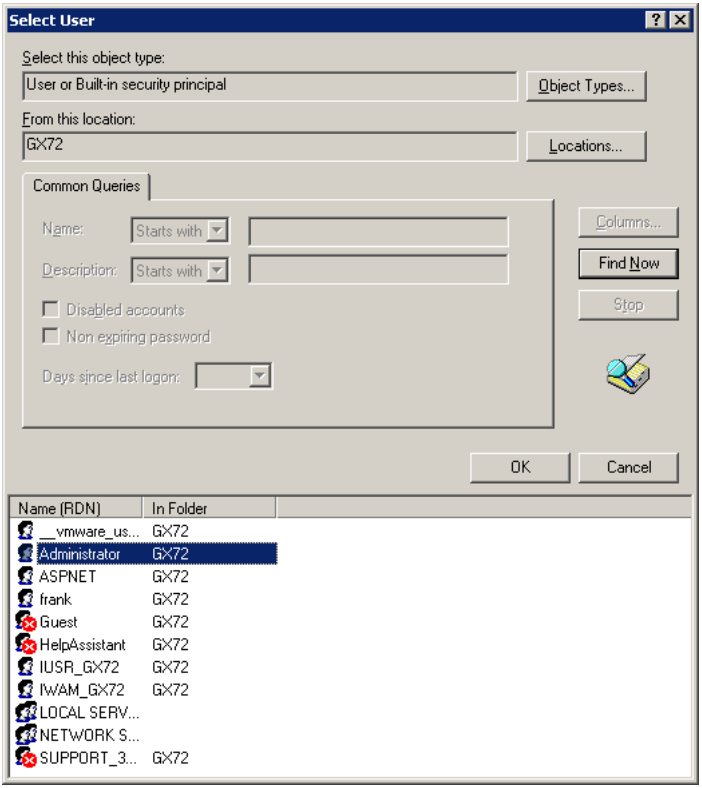


Abb. 26: Auswahl des Objektnamens

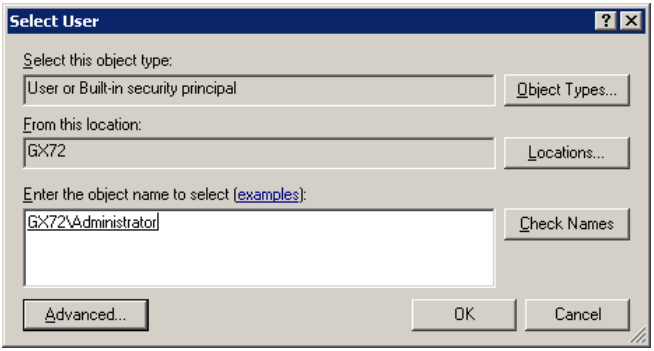


Abb. 27: Administrator Auswahl

Klicken Sie auf “Ok”, und tragen Sie das neue Passwort zweimal ein.

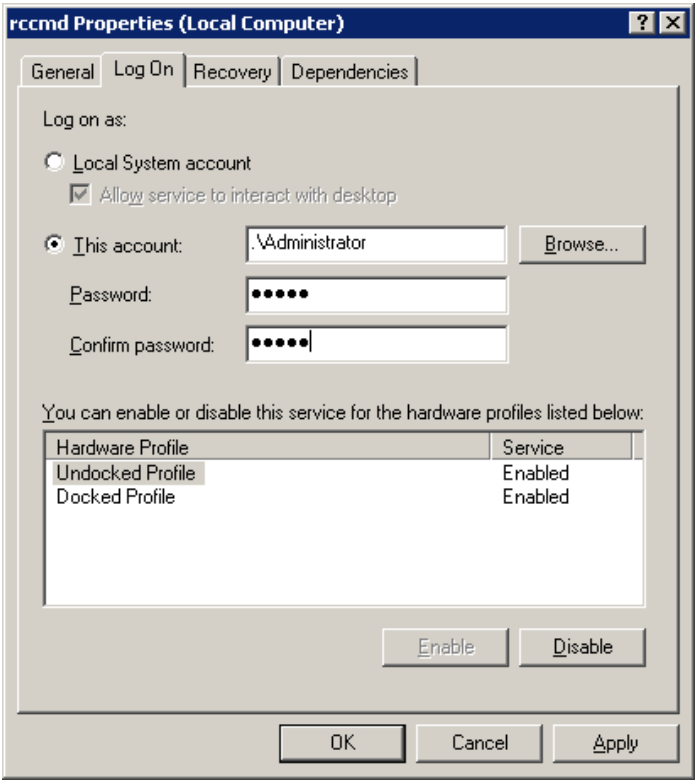


Abb. 28: Administrator Passwort Bestätigung

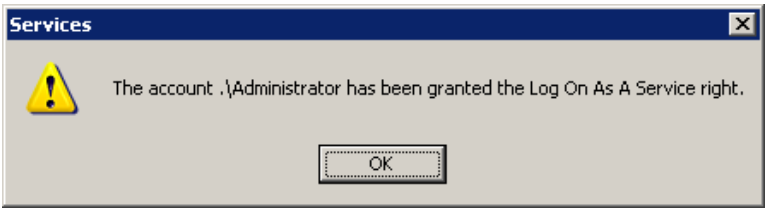


Abb. 29: Dienst-Berechtigungs-Fenster

3.5 Installation von RCCMD mit Redundanz (ab RCCMD V3)

Redundanz ist die Vervielfachung von kritischen Komponenten von einem System mit der Absicht, die Ausfallsicherheit zu maximieren. In den meisten sicherheitskritischen Systemen sind einige Teile der Kontrolleinheit verdreifacht. Ein Ausfall von einer Komponente würde von den anderen beiden kompensiert werden. Bei einer Dreier-Redundanz verfügt das System über drei Sub-Komponenten, die alle fehlerhaft sein müssten, bevor das System ausfällt. Die Wahrscheinlichkeit, dass drei Komponenten gleichzeitig ausfallen, ist ziemlich gering.

Bei der USV Installation bietet RCCMD eine Redundanz Management Funktion wie folgt an:

Jede USV muss mit einem CS121 oder einem UPSMAN Software Computer ausgestattet sein. Wenn Sie die Box “Use RCCMD group/redundancy” anhaken, gelangen Sie zu einem Menü, welcher CS121/UPSMAN diesen RCCMD Client versorgt. Z.B.: Wenn 4 CS121/UPSMAN in 4 USVen installiert sind, dann kann jeder ein Shutdown Signal zu diesem RCCMD Client absetzen.

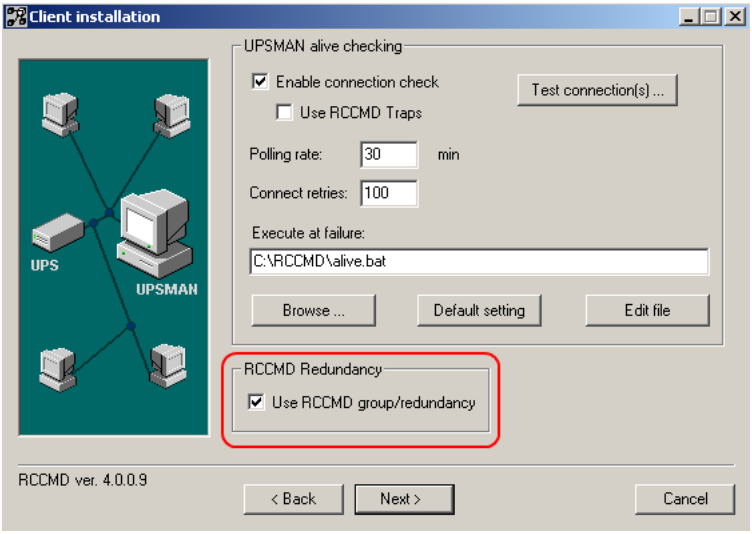


Abb. 30: Client Installation RCCMD Redundanz

Klicken Sie auf “Next”.

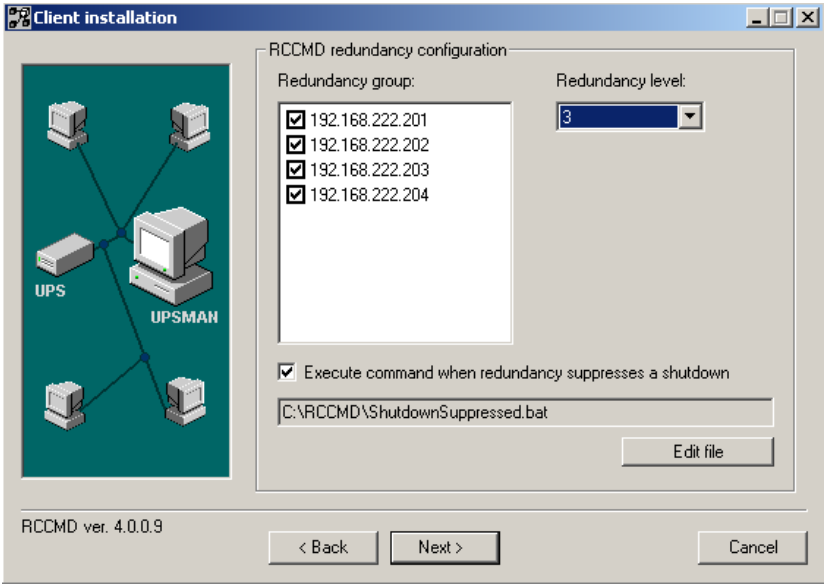


Abb. 31: Client Installation RCCMD Redundanz Konfiguration

Der Redundanz Level definiert, wieviele Shutdown Signale erforderlich sind, um das Shutdown.Bat File auszuführen. Solange diese Zahl nicht überschritten ist, wird der RCCMD Client Empfänger nur eine Pop-Up-Nachricht “Execute command when redundancy suppresses a shutdown” bringen. Das ist eine Information für den Benutzer, dass ein Shutdown von einem Gruppenmitglied empfangen wurde, aber das Signal unterdrückt wurde. Im obigen Beispiel würden 3 Shutdownsignale nur Nachrichten erzeugen, erst ein viertes Signal würde den Shutdown einleiten.

ACHTUNG: Bevor eine Shutdown-Suppressed-Nachricht abgesendet wird, überprüft RCCMD die Anwesenheit der anderen Gruppenmitglieder! Sollten diese nicht erreichbar sein, z.B. auf Grund von einem Netzwerkverlust, wird SOFORT ein Shutdown-Signal gesendet!

Inhalt von dieser Nachricht “ShutdownSuppressed.Bat”:

@echo off

start /b msg.exe -c:3

"Attention ! RCCMD Shutdown Signal received. Execution suppressed because of redundancy configuration. Please verify the status of the redundant UPS before you continue to work. NOTE: If the RCCMD shutdown sender problem has been solved, please stop/restart RCCMD service to reset the system. If you do not restart RCCMD

service the shutdown is still pending and will be activated if another RCCMD signal arrives !"

Wenn diese Nachricht erscheint, erwartet der RCCMD Client erst weitere Shutdown Signale, bis der Redundanzlevel erreicht ist. Ist dies der Fall, dann erst wird die Shutdown.Bat ausgeführt und das System heruntergefahren.

3.5.1 Automatisches Zurücksetzen des Redundanz Alarms

„Send RCCMD cancle shutdown“ kann verwendet werden, um automatisch einen vorher abgesendeten Shutdown zu verwerfen. Wenn ein Shutdown unterdrückt wurde, wegen der zu diesem Zeitpunkt noch vorhandenen Redundanz, das Problem aber zwischenzeitlich an der USV gelöst wurde, kann mittels einem „Send RCCMD cancel shutdown“ der Alarm zurückgesetzt werden. Durch diesen Befehl wird der RCCMD Client, der vorher das Shutdownsignal erhalten hat, aufgefordert, dieses wieder rückgängig zu machen.

Dieses Kommando kann indivduell in jedem Event/Alarm ihrer CS121 oder BACS WEBMANAGER Konfiguration eingefügt werden, macht allerdings nur dann Sinn, wenn der Event, der diesen Befehl absendet, auch tatsächlich dann aktiv ist, wenn die USV wieder als OK angesehen werden kann. Dafür geeignet sind Beispielsweise die Events „POWER RESTORED“, “BATTERY LOW OFF”, “UPSMAN STARTED” und “GENERAL ALARM OFF”, wenn diese in ihrem CS121 für diesen USV Typ angeboten werden. In diese „Entwarnungs-Ereignnisse“ würde dann der Job „Send RCCMD cancle shutdown“ eingetragen werden, sodass z. B. beim Neustart der USV, der Event „UPSMAN STARTED“ automatisch den betreffenden RCCMD Client wieder auf „normal“ zurücksetzt.

Alternativ: Sollte der Job „Send RCCMD cancle shutdown“ in ihrem CS121, UPSMAN oder BACS WEBMANAGER nicht vorhanden sein, kann alternativ auch der Job „Send RCCMD Command to remote client“ oder „Send RCCMD execute to remote client“ verwendet werden.

Der Parameter „WAKEUP“ hat die gleiche Funktion wie „Send RCCMD cancle shutdown“ und setzt den Redundanz Level eines RCCMD Clients in den Ausgangszustand zurück. Auch hier eignen sich die Events/Alarme POWER RESTORED, BATTERY LOW OFF, UPSMAN STARTED und GENERAL ALARM OFF besonders, um die Funktion „Send RCCMD Command to remote client“ mit dem „WAKEUP“ Befehl zu konfigurieren.

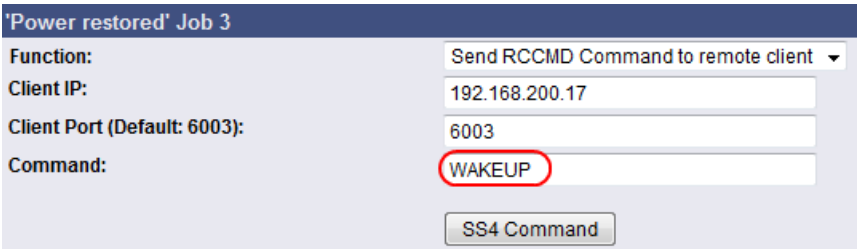


Abb. 32: CS121 Konfiguration „WAKEUP“ Befehl

Klicken Sie im CS121 Menü „Events/Alarms“ auf „Power restored“, und fügen Sie einen neuen Job hinzu. Wählen Sie die Funktion „Send RCCMD Command to remote client“ aus, tragen Sie die entsprechende IP-Adresse des Clients ein, und schreiben Sie den Befehl „WAKEUP“ in die „Command“ Zeile.

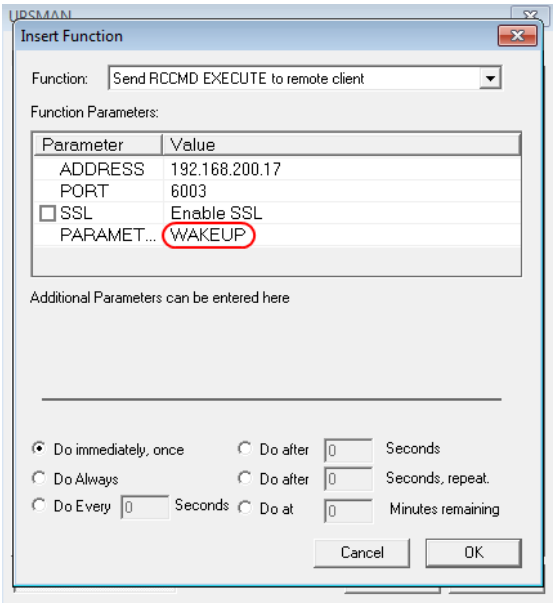


Abb. 33: UPSMAN Konfiguration „WAKEUP“ Befehl

Öffnen Sie die UPSMAN Konfiguration, und klicken Sie auf „Avanced Users“, „Events“, „Power restored“ und „Insert“. Fügen Sie die Funktion „Send RCCMD EXECUTE to remote client“ hinzu, und tragen Sie die entsprechende IP-Adresse des Clients ein, und schreiben Sie den Befehl „WAKEUP“ in die Parameter Zeile.

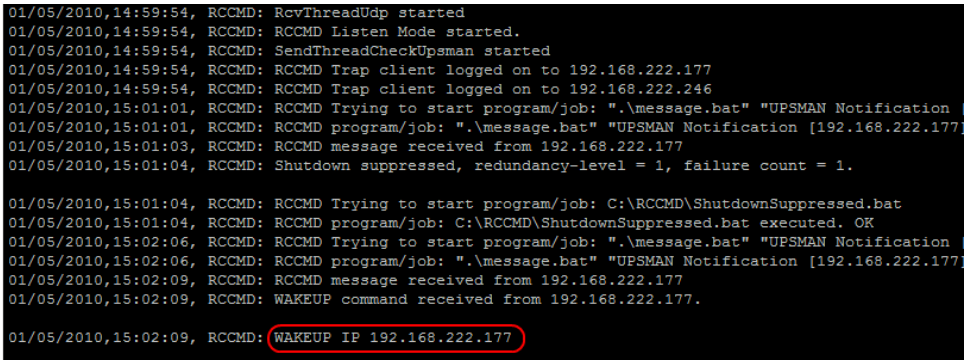

01/05/2010,14:59:54, RCCMD: RcvThreadUdp started
01/05/2010,14:59:54, RCCMD: RCCMD Listen Mode started.
01/05/2010,14:59:54, RCCMD: SendThreadCheckUpsman started
01/05/2010,14:59:54, RCCMD: RCCMD Trap client logged on to 192.168.222.177
01/05/2010,14:59:54, RCCMD: RCCMD Trap client logged on to 192.168.222.246
01/05/2010,15:01:01, RCCMD: RCCMD Trying to start program/job: ".\message.bat" "UPSMAN Notification
01/05/2010,15:01:01, RCCMD: RCCMD program/job: ".\message.bat" "UPSMAN Notification [192.168.222.177]
01/05/2010,15:01:03, RCCMD: RCCMD message received from 192.168.222.177
01/05/2010,15:01:04, RCCMD: Shutdown suppressed, redundancy-level = 1, failure count = 1.
01/05/2010,15:01:04, RCCMD: RCCMD Trying to start program/job: C:\RCCMD\ShutdownSuppressed.bat
01/05/2010,15:01:04, RCCMD: RCCMD program/job: C:\RCCMD\ShutdownSuppressed.bat executed. OK
01/05/2010,15:02:06, RCCMD: RCCMD Trying to start program/job: ".\message.bat" "UPSMAN Notification
01/05/2010,15:02:06, RCCMD: RCCMD program/job: ".\message.bat" "UPSMAN Notification [192.168.222.177]
01/05/2010,15:02:09, RCCMD: RCCMD message received from 192.168.222.177
01/05/2010,15:02:09, RCCMD: WAKEUP command received from 192.168.222.177.
01/05/2010,15:02:09, RCCMD: WAKEUP IP 192.168.222.177

Abb. 34: „WAKEUP“ Befehl im RCCMD Log

Hinweis: **Das Neustarten des RCCMD Dienstes ist eine dritte Möglichkeit, um den Redundanz Alarm zurückzusetzen.**

3.6 Der RCCMD Client als Relay Station

Wenn Sie eine grössere Anzahl von RCCMD Empfänger erreichen möchten, muss der CS121 Adapter als Relay Station fungieren. Der Empfänger wird so konfiguriert, dass er beim Erhalten eines RCCMD Signals eine Batch Datei startet, die weitere RCCMD Signale versendet. Diese Workstation ist dann Empfänger und Sender zur gleichen Zeit und somit eine wichtige Verbindung in der USV Überwachungskette. Der Gebrauch von einem RCCMD Client als Relay Station macht die Überwachung von mehreren hundert RCCMD Clients sehr viel einfacher als die Konfiguration über das Web-Interface des CS121. Außerdem haben alle Webbrowser Event Konfigurationen eine Sicherheits-limitierung, sodas es erforderlich ist, diese Relay Funktion zu nutzen, wenn die Anzahl der Jobs 50 pro Event auf dem CS121 HW131 übersteigt.

Sehen Sie in das folgende Script, das den RCCMD Client als Relay Station agieren lässt:

```
rem created by setup
@echo off
set path=%path%;C:\Program Files\RCCMD
# RELAY RCCMD
# This batch will send RCCMD shutdowns to the IP addresses listed below
# At the end of the batch this computer will initiate the local shutdown
start rccmd -s -a 192.168.200.2
start rccmd -s -a 192.168.200.3
start rccmd -s -a 192.168.200.4
start rccmd -s -a 192.168.200.5
start rccmd -s -a 192.168.200.6
start rccmd -s -a 192.168.200.7
# to be continued
#
# local shutdown
ExitWin.exe shutdown force
@cls
```

Abb. 35: Example: Batch File RCCMD als Relay Station

„start“ ist ein Windows Batchfile Kommando, um ein Programm-Aufruf in mehreren Instanzen zu starten. Dies ermöglicht das Ausführen von Programmen simultan und beschleunigt die Shutdown-Prozedur. Bitte beachten Sie, dass „start“ nicht auf allen Windows OS unterstützt wird und sollte getestet werden, bevor es verwendet wird.

Ab der RCCMD Version 4.0.1.0 ist auch eine grafische Konfiguration im RCCMD Wizard für die Relay Funktion enthalten.

Klicken Sie in der Client Installation auf “Configure…”.

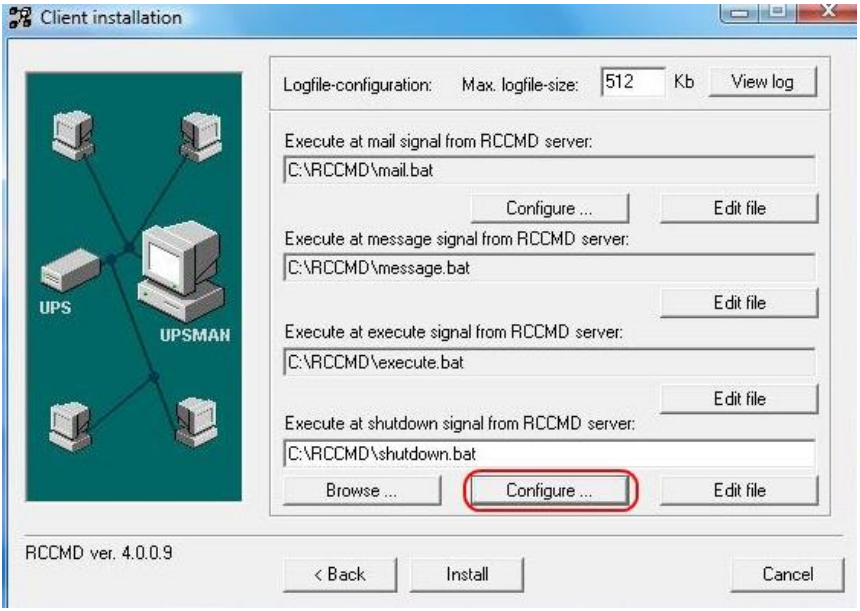


Abb. 36: RCCMD Client Shutdown Konfiguration

Markieren Sie im “Available Commands” Fenster das “RCCMD shutdown relay”, und klicken Sie auf den Pfeil “>”, um diese Funktion der “Current Sequence” hinzuzufügen.

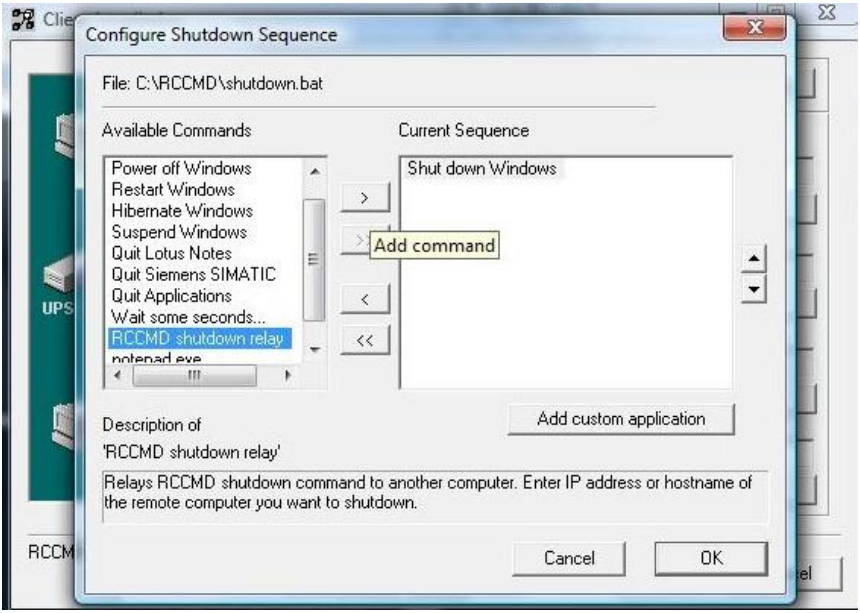


Abb. 37: RCCMD Shutdown Relay

Es öffnet sich das folgende Fenster, in dem man den gewünschten IP-Adressen-Bereich eingeben kann oder eine einzelne IP-Adresse.

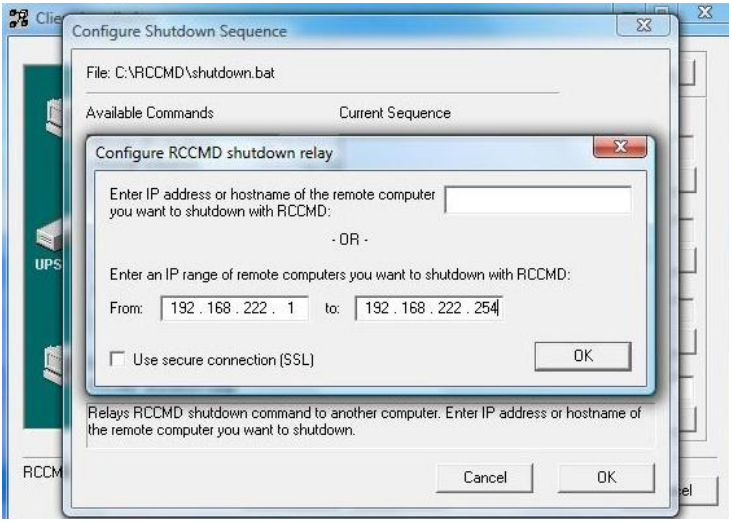

Configure Shutdown Sequence
File: C:\RCCMD\shutdown.bat
Available Commands
Current Sequence
Configure RCCMD shutdown relay
Enter IP address or hostname of the remote computer you want to shutdown with RCCMD:
- OR -
Enter an IP range of remote computers you want to shutdown with RCCMD:
From: 192 . 168 . 222 . 1
to: 192 . 168 . 222 . 254
Use secure connection (SSL)
OK
Relays RCCMD shutdown command to another computer. Enter IP address or hostname of the remote computer you want to shutdown.
Cancel
OK

Abb. 38: RCCMD Konfiguration IP-Adressen-Bereich

Ausserdem kann man hier auch die SSL-Funktion aktivieren (siehe auch Kapitel 3.9).

Um einzelne IP-Adressen aus dem Bereich zu entfernen, markieren Sie die Zeile mit der gewünschten Adresse, und klicken Sie auf den Pfeil “<”.

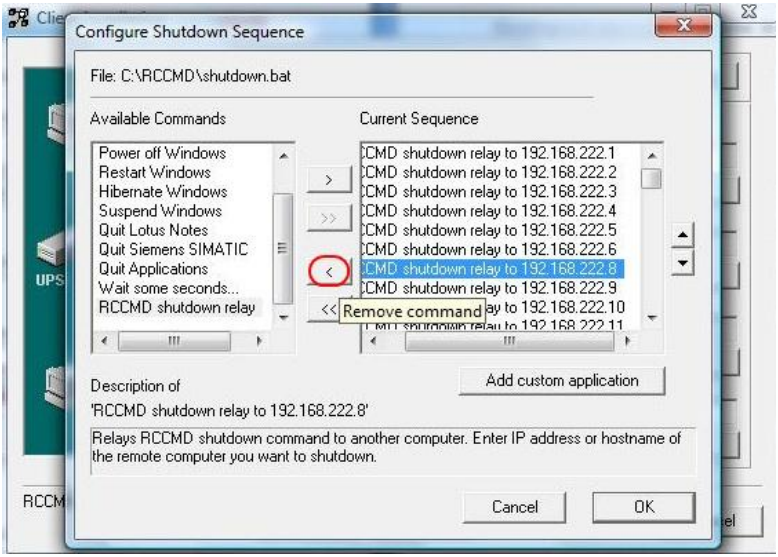


Abb. 39: RCCMD Shutdown Relay Adress-Entfernung

Das Ergebnis der grafischen Konfiguration von einem RCCMD Relay befindet sich in dem Shutdown-Skriptfile „shutdown.bat“.

```
@ECHO off
REM --- Created by RCCMD configuration ---
SET path=%path%;C:\Program Files\RCCMD
rccmd.exe -s -a 192.168.200.10
rccmd.exe -s -a 192.168.200.11
rccmd.exe -s -a 192.168.200.12
rccmd.exe -s -a 192.168.200.13
rccmd.exe -s -a 192.168.200.14
rccmd.exe -s -a 192.168.200.15
rccmd.exe -s -a 192.168.200.16
rccmd.exe -s -a 192.168.200.17
rccmd.exe -s -a 192.168.200.18
rccmd.exe -s -a 192.168.200.19
rccmd.exe -s -a 192.168.200.20
ExitWin.exe shutdown force
@CLS
```

Abb. 40: RCCMD Shutdown Relay in der „Shutdwown.bat“

Der Unterschied zu der o.g. Beschreibung der Shutdown-Sequenz ist, dass das grafische Tool nicht den „start“ Parameter verwendet und dadurch der Shutdown die Signale nacheinander versendet. Jede IP-Adresse, die auf diesen RCCMD Call nicht antwortet, benötigt 10 Sekunden (default) bis der Timeout erreicht ist und das nächste Kommando ausgeführt wird.

3.7 RCCMD auf Windows 95/98

RCCMD für Windows 95/98 funktioniert so, wie RCCMD auf Windows NT. Der einzige Unterschied ist der Programmname, nämlich RCCMD95.EXE. Bitte schauen Sie auch in den Windows Abschnitt von diesem Handbuch.

Achtung: **Für Windows 95/98 Benutzer empfehlen wir die Installation von dem TCP/IP Protokoll, bevor Sie die Installation des RCCMD Wizard starten.**

Achtung: **Wenn Sie WINPOP.EXE benutzen, können Sie RCCMD nicht auf dem Port 6003 starten. Bitte verändern Sie die Sender und Empfänger dementsprechend.**

Erfahrene Anwender sollten den Registry Editor nutzen und alle Veränderungen manuell vornehmen. Unerfahrene Anwender sollten den RCCMD Wizard benutzen.

Registry Einstellungen: Bitte überprüfen Sie Folgendes: Wenn Sie den RCCMD Prozess im Lauscher-Modus nutzen möchten, müssen Sie die folgenden Parameter in der Register Datenbank eintragen:

regedit.exe rccmd95.reg or simply start rc_init.bat

Die Parameter befinden sich nun im folgenden Register:

HKEY_LOCAL_MACHINE\CurrentControlSet\Services\RCCMD95\Parameters

Starten Sie die Regedit.Exe, wenn Sie RCCMD umkonfigurieren möchten.

Wenn Sie mit dem Register Editor von Windows 95 nicht vertraut sind, können Sie anstelle die RCCMD95.EXE modifizieren. Führen Sie die Regedit.Exe und die RCCMD.EXE aus:

Parameter:

***Port:* Spezieller TCP-Port, der das RCCMD Signal empfängt.**

***Addr1... 10*: TCP/IP Adresse von der Workstation, die das RCCMD Signal akzeptiert.**

***ExecutePrg*: Der Befehl, der beim empfang des RCCMD Signals ausgeführt wird.**

Um RCCMD zu starten, führen Sie diesen Befehl aus:

rccmd95

Oder starten Sie das Programm mit Hilfe der Startmenü-Leiste.

Um RCCMD im Sender Modus auszuführen, tragen Sie bitte die folgenden Parameter in Ihrem Shutdown-Job ein:

RCCMD95 -s -a <address> [-p 6003]

Mit <address> ist die IP-Adresse der Workstation gemeint, der Sie das RCCMD Signal senden möchten.

Optionale Parameter:

-p <port> = TCP-Port, zu dem das RCCMD Signal gesendet wird.

Die Option –a kann mehrere Male genutzt werden, wenn ein Shutdown auf mehreren Remote Computern ausgeführt werden soll.

Nutzen Sie die RCCMD CD-Lizenz nicht mehr als einmal (siehe Copyright, Seite 1). Wenn mehr als ein RCCMD Modul installiert werden muss, um einen Shutdown auszuführen, müssen Sie weitere Lizenzen bestellen, die Sie bei Ihrem USV Händler erhalten können.

3.8 RCCMD auf Windows NT/2000/XP/2003/2008

Das RCCMD (Remote Console Command) ist ein Programm, das die Ausführung von Programmen auf Remote Computer ermöglicht. Dieses Tool ist Teil von allen UPSMAN unterstützten Betriebssystemen, mit der Ausnahme von Windows 3.x. Dieses Tool bietet

die Möglichkeit, Verbindungen zwischen verschiedenen Betriebssystemen herzustellen. Wenn die UPS Management Software auf einer Windows NT/2000/XP Maschine installiert ist und ein Remote Shutdown auf einer Remote Maschine ausgeführt werden soll, auf dem ein anderes Betriebssystem läuft, werden Sie das RCCMD Tool benötigen.

Das RCCMD Tool arbeitet in zwei verschiedenen Modi. Das Modul arbeitet wie ein normales Programm, im Sender Modus, um RCCMD Befehle zu anderen Workstations zu senden, im Lauscher Modus, der als NT Dienst im Hintergrund läuft und auf Befehle wartet.

Achtung: **Für unerfahrene Anwender empfehlen wir das Ausführen des RCCMD Wizard, der die Konfiguration erleichtert. Starten Sie den Wizard von Ihrer entsprechenden Programm Gruppe.**

Attention: **Bitte benutzen Sie den Wizard und die Manuelle Konfiguration nicht zur gleichen Zeit.**

Eventuell benötigen Sie zum einwandfreien Ausführen von RCCMD besondere Privilegien, um Befehle und Programme auszuführen. Die RCCMD Start Parameter müssen in der Systemsteuerung auf den Administrator/Superuser mit dem korrekten Passwort eingetragen sein. Wenn Sie nicht authorisiert sind, den Admin Zugang zu benutzen, muss ein neuer Zugang eingerichtet werden, der die Berechtigung hat, diese Workstation herunterzufahren. Setzen Sie in der Systemsteuerung die RCCMD Start Parameter auf “This Account” und tragen Sie den “Any Administrative Account” ein.

Nun wurde RCCMD erfolgreich installiert und ist in der Lage, die C:\ups\shutdown.bat auszuführen.

3.9 RCCMD auf Windows 2008 Server Core x64

Bei der Konfiguration von RCCMD auf Windows 2008 Server Core x64 gibt es die Besonderheit, dass die RCCMD Konfiguration aus dem Standardverzeichnis C:\RCCMD mit dem folgenden Befehl aufzurufen ist:

```
C:\RCCMD>RCCNF_NT.EXE
```

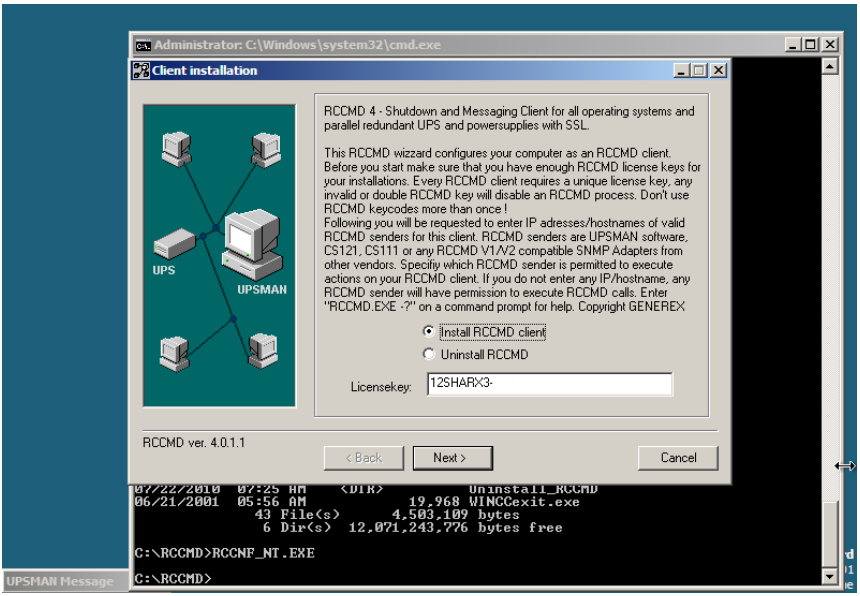

Administrator: C:\Windows\system32\cmd.exe
Client installation
RCCMD 4 - Shutdown and Messaging Client for all operating systems and parallel redundant UPS and powersupplies with SSL.
This RCCMD wizzard configures your computer as an RCCMD client. Before you start make sure that you have enough RCCMD license keys for your installations. Every RCCMD client requires a unique license key, any invalid or double RCCMD key will disable an RCCMD process. Don't use RCCMD keycodes more than once !
Following you will be requested to enter IP adresses/hostnames of valid RCCMD senders for this client. RCCMD senders are UPSMAN software, CS121, CS111 or any RCCMD V1/V2 compatible SNMP Adapters from other vendors. Specifiy which RCCMD sender is permitted to execute actions on your RCCMD client. If you do not enter any IP/hostname, any RCCMD sender will have permission to execute RCCMD calls. Enter "RCCMD.EXE -?" on a command prompt for help. Copyright GENEREX
Install RCCMD client
Uninstall RCCMD
Licensekey:
12SHARX3-
UPS
UPSMAN
RCCMD ver. 4.0.1.1
< Back
Next >
Cancel
06/21/2001 05:56 AM 19,968 WINCCexit.exe
43 File(s) 4,503,109 bytes
6 Dir(s) 12,071,243,776 bytes free
C:\RCCMD>RCCNF_NT.EXE
C:\RCCMD>
UPSMAN Message

Abb. 41: RCCMD Konfiguration

Schauen Sie bitte in das Kapitel 3 auf Seite 7 für den Installationsablauf und der Konfiguration von RCCMD.

3.10 RCCMD mit SSL auf Windows

Das *Secure Sockets Layer* (SSL) Protokoll ist ein kryptografisches Protokoll, das Sicherheit und Datenintegrität für Kommunikationen in TCP/IP Netzwerken zusätzlich bietet. Bei einem Versand von RCCMD Nachrichten wird dann eine Verschlüsselung (auch mit eigenen Zertifikaten) verwendet und nur dann auf dem Client ausgeführt, wenn die Codes übereinstimmen und sich auch in einem gewissen Zeitrahmen (Zeitstempel) befinden.

Stellen Sie über einen Webbrowser eine Verbindung zum CS121 SNMP Adapter her. Klicken Sie im Konfigurations-Menü auf “Network & Security”, und setzen Sie den Haken bei “Use RCCMD SSL”.

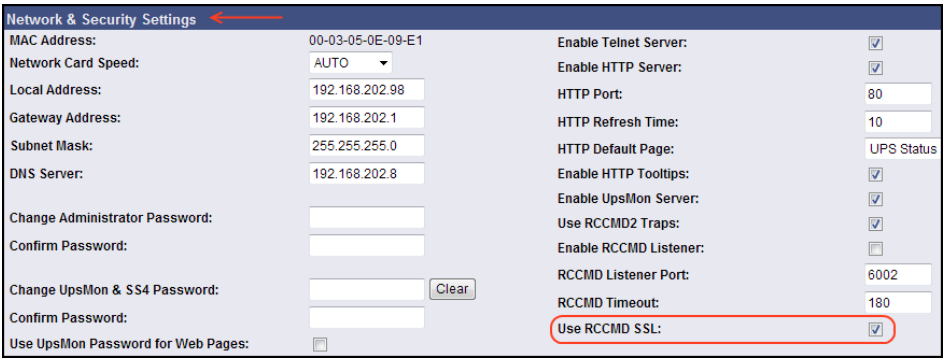


Abb. 42: RCCMD SSL Einstellung

Das SSL Netzwerk Feature erfordert einen korrekten Zeitstempel. Konfigurieren Sie im „Timeserver“ Menü eine entsprechende IP-Adresse.

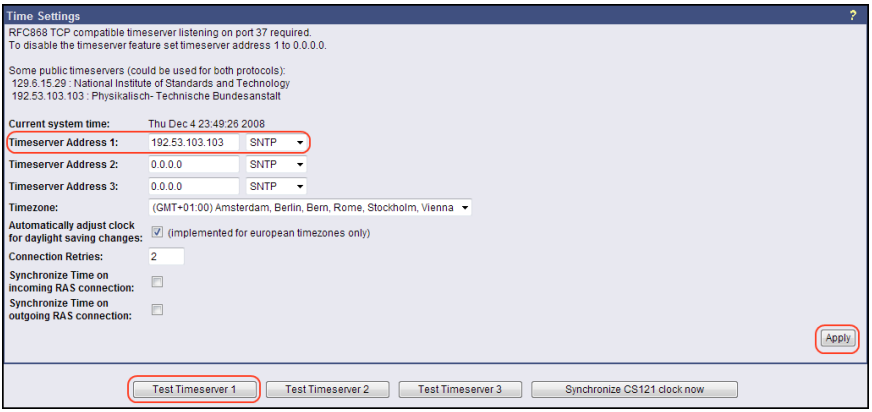


Abb. 43: Timeserver Konfiguration

Klicken Sie auf das „Save Configuration“ Menü, und bestätigen Sie Ihre Einstellungen mit „Save, Exit & Reboot“.

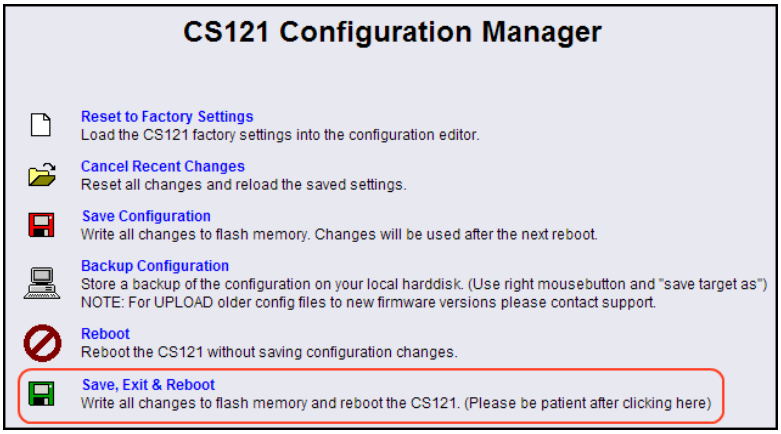

CS121 Configuration Manager
Reset to Factory Settings
Load the CS121 factory settings into the configuration editor.
Cancel Recent Changes
Reset all changes and reload the saved settings.
Save Configuration
Write all changes to flash memory. Changes will be used after the next reboot.
Backup Configuration
Store a backup of the configuration on your local harddisk. (Use right mousebutton and "save target as")
NOTE: For UPLOAD older config files to new firmware versions please contact support.
Reboot
Reboot the CS121 without saving configuration changes.
Save, Exit & Reboot
Write all changes to flash memory and reboot the CS121. (Please be patient after clicking here)

Abb. 44: Speichern der Einstellungen

Starten Sie die RCCMD Wizard Installation erneut, und aktivieren Sie das SSL Feature.

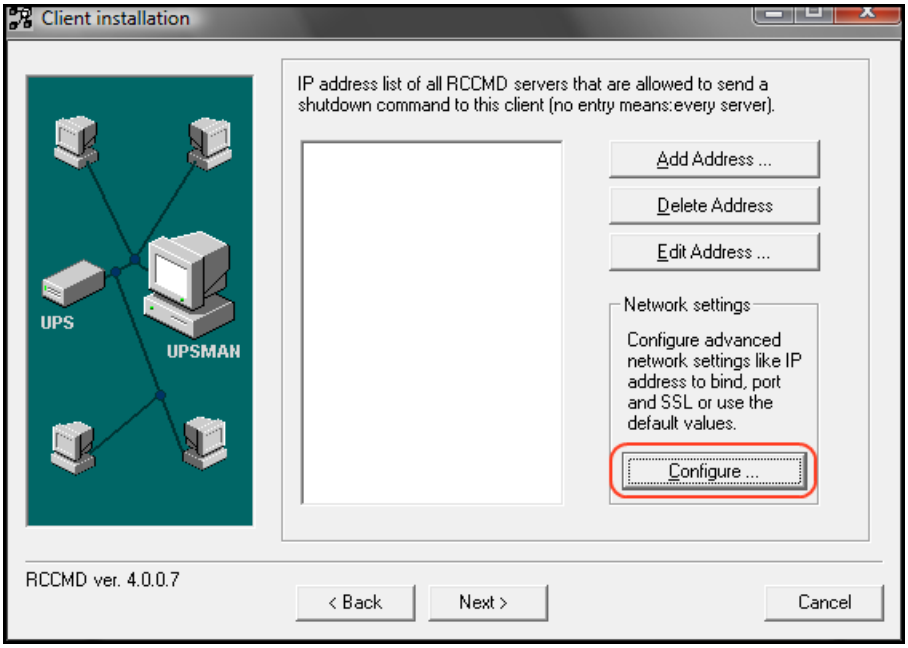

Client installation
IP address list of all RCCMD servers that are allowed to send a shutdown command to this client (no entry means:every server).
Add Address ...
Delete Address
Edit Address ...
Network settings
Configure advanced network settings like IP address to bind, port and SSL or use the default values.
Configure ...
UPS
UPSMAN
RCCMD ver. 4.0.0.7
< Back
Next >
Cancel

Abb. 45: SSL Konfiguration

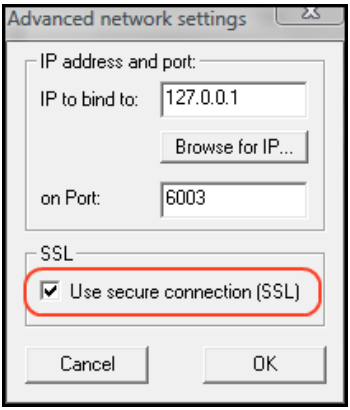


Abb. 46: Advanced Network Settings

Alternative Konfiguration mit einem ASCII-Editor

Sie können die gewünschte Konfiguration mit einem ASCII-Editor manuell in die Konfigurationsdatei „rccmd.cfg“ eintragen.

```
##########################################
# RCCMD Configuration (v3-default)
##########################################

#
# Bind on Interface
# Defines on which interface we listen for incoming commands
# Default: 0.0.0.0 (All possible interfaces on this host)
#
ListenAddress=0.0.0.0

#
# Listen on Port
# Defines on which interface port we listen for incoming commands.
# Default: 6003
#
```

```
ListenPort=6003

#
# Enable UDP
# Defines if we should listen for rccmd (UDP) broadcasts
# Default: true
#
ListenUDP=true

#
# Access Control List
# A list of valid sender addresses, only its members can connect to us.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (Everyone is allowed to connect to us)
#
AllowedAddresses=

########################################
# Alive Check
#
# Enable Alive Check
# Defines if we should perform UPSMan alive checking.
# Default: false
#
AliveEnabled=false

#
# Alive Check Rate
# Defines the interval of UPSMan alive checking, in seconds.
```

```
# Default: 1800
#
AliveInterval=1800

#
# Alive Retry Rate
# Defines the number of UPSMan alive checking retries, in case of problems.
# Default: 0
#
AliveRetries=5

#
# Alive Check Group Members List
# A list of UPS device addresses that should be checked periodically.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (No alive checking)
#
AliveAddresses=

#
# Alive Program
# Full path to script that is executed when an alive check fails.
# Default: rccmd_notalive.sh
#
AliveProg=

########################################
# Redundancy Mode
#
```

```
# Enable Redundancy
# Defines if we should operate in redundancy mode.
# Requires an enabled <Alive Check> configuration.
# Default: false
#
RedundancyEnabled=false

#
# Redundancy Group Members List
# A list of redundancy group member addresses, must be also in <AliveAddresses>.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (No redundancy available)
#
RedundancyAddresses=

#
# Redundancy Level
# Defines how many of the <RedundancyAddresses> are redundant.
# Shutdown is executed when the number of shutdown requests exceeds this number.
# Default: 0 (No redundancy available)
#
RedundancyLevel=0

# Enable Redundancy Script
# Defines if we should NOT execute a script when redundancy suppresses a shutdown.
# Default: false.
#
RedundancyBatchSuppress=false
```

Redundancy Script

Full path to script that is executed when redundancy suppresses a shutdown.

Default: ShutdownSuppressed.sh

#

RedundancyBatchFile=

##

Sie können während der Installation die grafische Konfiguration überspringen und gleichzeitig eine kommentierte „rccmd.cfg“ erzeugen, wenn Sie die Frage:

```
This is NOT an ITANIUM (IA-64) system [Y/n]?:
```

mit „n“ beantworten.

3.10.1 RCCMD mit eigenen SSL Zertifikaten

In diesem Abschnitt beschreiben wir, wie man ein eigenes SSL Zertifikat mit RCCMD nutzen kann, z. B. OpenSSL (http://www.openssl.org/related/binaries.html):

Erstellung eigener Zertifikate (CA)

Mit der Nutzung von OpenSSL ist es sehr einfach, sein eigener Zertifizierer zu werden. Nutzen Sie einfach diesen Befehl:

```
CA.pl –newca
```

Fertig! Vergewissern Sie sich, dass Sie einen gebräuchlichen CN (gewöhnlichen Namen) verwendet haben.

Erstellen des RCCMD Zertifikats

Nun müssen Sie Ihr Zertifikat für RCCMD erstellen. Da es für die Verifizierung den CN nutzt, sollte das Zertifikat diesen Namen auch enthalten, den Sie für das CA gewählt haben. Die private Schlüssel muss nicht verschlüsselt werden, um den RCCMD Client (Dienst) zu starten. Dafür nutzen wir die “-nodes” Option und den “-newreq” Befehl:

```
CA.pl –newreq -nodes
```

Signieren mit CA:

```
CA.pl –sign
```

Erstellen Sie nun eine leere Datei mit dem Namen “rccmd.pem”, und kopieren Sie die Zertifizierungsinformationen von “newcert.pem” (RCCMD Zertifikat), “newkey.pem” (Privater Schlüssel) und “cacert.pem” (CA) in diese Datei. Bitte beachten Sie, dass das exakte Kopieren erforderlich ist, damit Sie es ohne Probleme nutzen können.

Nutzung des eigenen RCCMD Zertifikats

Führen Sie die folgenden Schritte auf jedem RCCMD Client und Sender aus, um die Konfiguration abzuschliessen.

- Stellen Sie ein Backup von der existierenden “rccmd.pem” her
- Ersetzen Sie die “rccmd.pem” mit Ihrer eigenen
- Starten Sie den RCCMD Client neu
- Starten Sie den RCCMD Sender neu

3.11 Testen der RCCMD Verbindung

Testen Sie letztendlich Ihre Konfiguration, wenn alle RCCMD Clients vorhanden sind. Führen Sie RCCMD im Debug Modus aus (RCCMD –debug –s/l-a). Senden Sie ein Echo (Ping) zu jedem Remote Client mit dem Befehl “ping [hostname][IP-Adresse]”. Wenn der Ping beantwortet wird, können Sie nun den RCCMD Verbindungs-Test im Debug-Modus starten. Wenn alles funktioniert, können Sie sehen, dass eine Verbindung aufgebaut und wieder geschlossen wurde. Das bedeutet, dass der Remote RCCMD Client Ihr Signal empfangen hat und das Shutdown script remote ausführen wird.

ACHTUNG! Dieser Test wird das Shutdown Script ausführen! Wenn Sie den Shutdown vermeiden möchten, sollten Sie den Shutdown-Befehl aus dem RCCMD Client Shutdown.Bat/SH File herausnehmen.

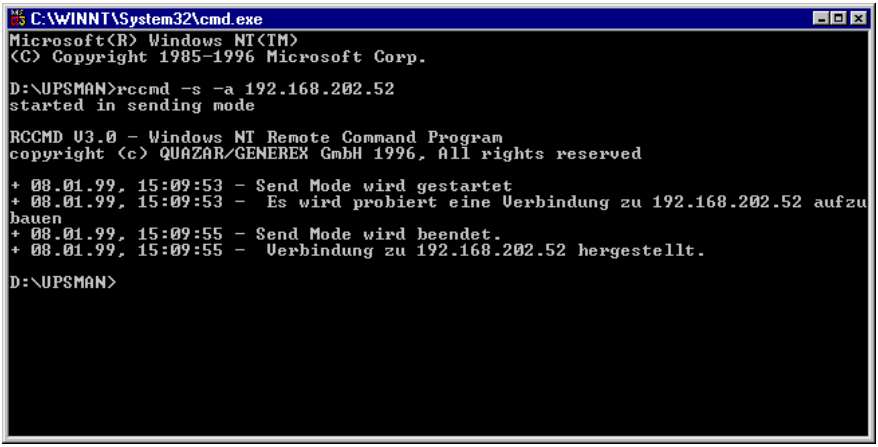

C:\WINNT\System32\cmd.exe
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.
D:\UPSMAN>rccmd -s -a 192.168.202.52
started in sending mode
RCCMD V3.0 - Windows NT Remote Command Program
copyright (c) QUAZAR/GENEREX GmbH 1996, All rights reserved
+ 08.01.99, 15:09:53 - Send Mode wird gestartet
+ 08.01.99, 15:09:53 - Es wird probiert eine Verbindung zu 192.168.202.52 aufzu
bauen
+ 08.01.99, 15:09:55 - Send Mode wird beendet.
+ 08.01.99, 15:09:55 - Verbindung zu 192.168.202.52 hergestellt.
D:\UPSMAN>

Abb. 47: RCCMD Konsolen-Test

3.11.1 Testen der RCCMD 2 Verbindung

Um zu überprüfen, ob der UPSMAN Prozess unter RCCMD 2 auf dem Remote Client aktiv ist, nutzen Sie folgende Syntax:

rccmd –sc –ac <IP address>

```
C:\RCCMD>rccmd -sc -ac 192.168.222.201
started in sending mode

RCCMD V4.0.0.7 - Windows NT Remote Command Program
Copyright (c) 1996-2007 Generex GmbH

RCCMD Send Mode started
RCCMD  Upsman at 192.168.222.201 alive.
RCCMD Send Mode stopped

C:\RCCMD>_
```

Abb. 48: RCCMD Alive Check via Befehlszeile

Wenn der UPSMAN aktiv ist, erhalten Sie die Nachricht “UPSMAN <IP-Adresse> alive”. Sie werden keine Nachricht erhalten, wenn der Dienst inaktiv ist.

Testen Sie die RCCMD 2 Verbindung mit der “Alive Check” Option im RCCMD Wizard: Wenn Sie die “UPSMAN alive checking” Funktion nutzen möchten (empfohlen), setzen Sie einen Haken in der “Enable connection check” Box. Der Alive Check ist ein Signal, das zum UPSMAN oder CS121 über den Port 5769 gesendet wird, um zu prüfen, ob der UPSMAN über USV Daten verfügt oder nicht.

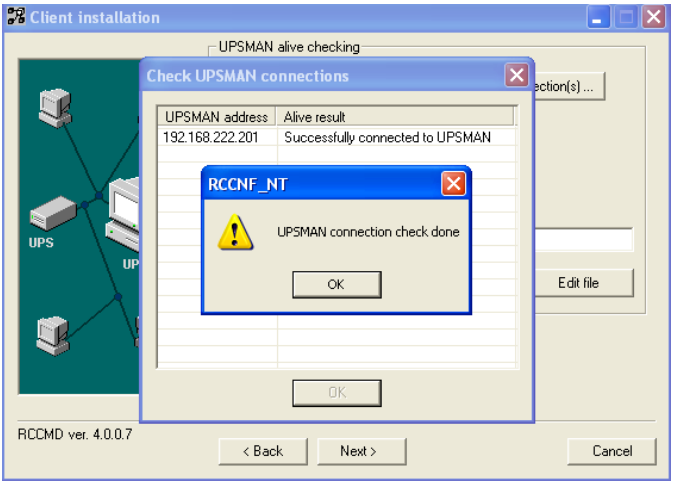


Abb. 49: UPSMAN Alive Check Fenster

Benutzen Sie diesen Befehl, um die RCCMD-Hilfe aufzurufen: C:\Program Files\RCCMD>rccmd -?

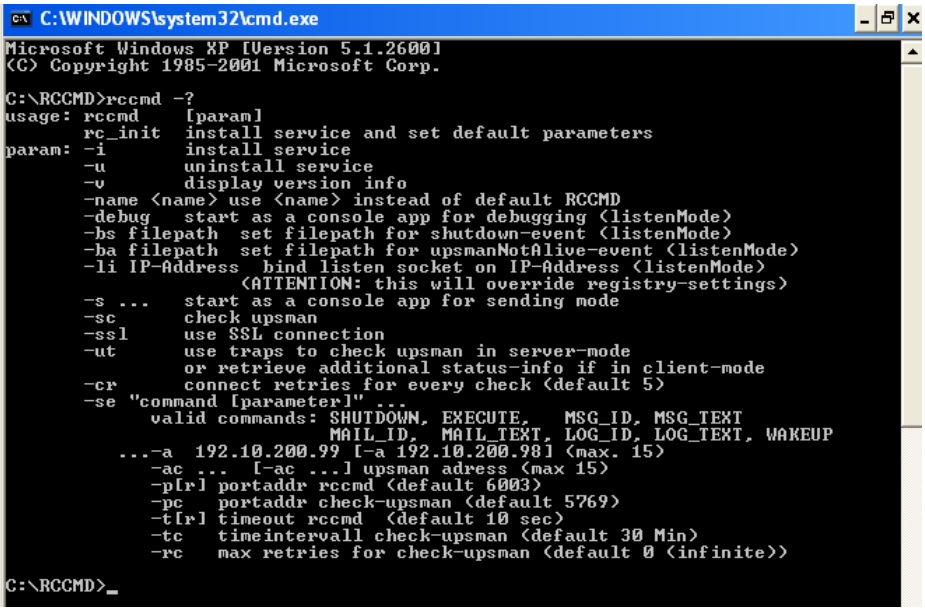

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\RCCMD>rccmd -?
usage: rccmd [param]
rc_init install service and set default parameters
param: -i install service
-u uninstall service
-v display version info
-name <name> use <name> instead of default RCCMD
-debug start as a console app for debugging (listenMode)
-bs filepath set filepath for shutdown-event (listenMode)
-ba filepath set filepath for upsmanNotAlive-event (listenMode)
-li IP-Address bind listen socket on IP-Address (listenMode)
(ATTENTION: this will override registry-settings)
-s ... start as a console app for sending mode
-sc check upsman
-ssl use SSL connection
-ut use traps to check upsman in server-mode
or retrieve additional status-info if in client-mode
-cr connect retries for every check (default 5)
-se "command [parameter]" ...
valid commands: SHUTDOWN, EXECUTE, MSG_ID, MSG_TEXT
MAIL_ID, MAIL_TEXT, LOG_ID, LOG_TEXT, WAKEUP
...-a 192.10.200.99 [-a 192.10.200.98] (max. 15)
-ac ... [-ac ...] upsman adress (max 15)
-p[r] portaddr rccmd (default 6003)
-pc portaddr check-upsman (default 5769)
-t[r] timeout rccmd (default 10 sec)
-tc timeintervall check-upsman (default 30 Min)
-rc max retries for check-upsman (default 0 (infinite))
C:\RCCMD>

Abb. 50: RCCMD Konsole -?

4. RCCMD auf NovellNetWare

Wenn Sie den Hilfs-Parameter “?” auf einer NovellNetWare Konsole eingeben, erhalten Sie folgende Hinweise:

```
Possible parameters:

 -l
     listen. waits for a command from RCCMD sender

 -s
     sends a ping to a listening program

 -se <command> <param>
     sends a command to a listening program

 -p  <port>
     Portadress (Defaultadress = 6003)

 -a  <ipaddress>
     Address in IP Format. Ex. -a 192.10.20.30 (max.
10)

 -t  <timeout>
     Time in Seconds (Defaulttimeout = MAX_TIMEOUT)
```

```
 -?
     this help

Supported Commands (for use with -se argument):

 SHUTDOWN
          This will call the configured shutdown-
batchfile (default: shutdown.bat)

 EXECUTE
          This will call the execute.bat file

 MSG_TEXT
          This will call the message.bat file
<text, unrestricted word count>

 MSG_ID <ID>
          This will call the message.bat file
<message parameters, seperated by blanks>

 LOG_TEXT
          This will write to configured log-file
(default: rccmd.log) <text, unrestricted word count>

 LOG_ID <ID>
          This will write to configured log-file
(default: rccmd.log) <message parameters, seperated
by blanks>

Examples:

 load rccmd.nlm -s -a 192.10.200.52 -a 192.10.200.53
 load rccmd.nlm -s -a 192.10.200.52 -a 192.10.200.53
-t 10
 load rccmd.nlm -se "SHUTDOWN" -a 192.10.200.52

 load rccmd.nlm -se "EXECUTE" -a 192.10.200.52
 load rccmd.nlm -se "MSG_TEXT this is a message" -a
192.10.200.52
 load rccmd.nlm -l
 load rccmd.nlm -l -a 192.10.200.52 -a 192.10.200.53
 load rccmd.nlm -l -a 192.10.200.52

If you have added a search path i.e.: "search add
sys:rccmd",
```

otherwise you have to use the absolute path.

```
load sys:rccmd\rccmd.nlm -l
```

Um RCCMD im Lauscher Modus zu starten, geben Sie bitte Folgendes ein:

load <path> RCCMD -l [-a 192.200.100.10] [-p 6003] load <path> shutcmd.nlm –f

Optionale Parameter:

-a <address> TCP/IP Adresse vom RCCMD Master, der das Signal sendet

-p <port> (optional) TCP-Port Adresse, auf den der Master das Signal sendet

Um RCCMD im Sender Modus zu starten, tragen Sie Folgendes in Ihren Shutdown-Job ein:

load RCCMD -s -a <address> [-p 6003]

Tragen Sie die IP-Adresse der Workstation ein, der Sie das Signal senden möchten (Workstations im Lauscher Modus mit einem aktiven RCCMD)

Optionale Parameter:

-p <port> TCP-Port, der das RCCMD Signal nutzt

Die Option "-a" kann mehrmals verwendet werden, wenn ein Shutdown auf Remote Netzwerk Servern ausgeführt werden soll.

Beispiel: (Pfad <path> = sys:\ups\upsman\rccmd.nlm)

load <path> RCCMD.NLM –s –a 192.168.210.3 -a 192.168.210.4 -a 192.168.210.10

...etc. bis unendlich

unload RCCMD

load <path> RCCMD.NLM –s –a 192.168.210.8...etc.

unload RCCMD

Bitte benutzen Sie den Lizenzschlüssel nicht mehr als einmal. Wenn Sie mehrere RCCMD Module für Shutdowns installieren möchten, benötigen Sie weitere Lizenzen, die Sie bei Ihrem USV Händler erhalten können.

rccmd.nlm

Modul für den Multiserver Shutdown in IP-Netzwerken. Das RCCMD.NLM beinhaltet verschiedene Befehlszeilen Parameter, die entweder im Sender Modus oder im Lauscher Modus verwendet werden:

rccmd -? Help

rccmd -s Sending off a "ping" signal to a waiting program

rccmd -l Waiting for a ”ping” signal. A command can be executed after the reception of the ”ping” signal.

rccmd –p Setting the port address (default = 6003).

rccmd –a Address in IP format e.g. 192.168.202.1

rccmd –t Time in seconds until a connection will be established. (default timeout = 10)

Example:

load sys:ups\rccmd.nlm -s -a 192.168.202.1 [-a 192.168.202.1]

load sys:ups\rccmd.nlm -s -a 192.168.202.1 -t 10

load sys:ups\rccmd.nlm -l -a 192.168.202.1 shutcmd.nlm [/para]

rccmdipx.nlm

Dies ist ein Modul speziell für IPX Netzwerke. Das Modul sendet einen Shutdown Befehl (oder jeden anderen Konsolen Befehl) direkt zu jeden IPX Server Namen. Bitte starten Sie RCCMDIPX auf allen Novell Konsolen. Das Modul muss auf beiden Servern geladen werden:

Benennen Sie die Datei um von RCCMDIPX zu RCCMS.NLM 2. Laden Sie RCCMD wie folgt:

rccmd <server name> <console command>

Als Servername muss ein gültiger Name aus der Netzwerk Umgebung angegeben werden, als Befehl ein gültiger NetWare-Befehl.

Beispiel:

1. load sys:ups\rccmdipx (or load RCCMD if RCCMDIPX.NLM is renamed to RCCMD.NLM)

2. rccmd gnw1 forcedown

or 1. load sys:ups\rccmdipx

2. rccmd gnw1 sys:ups\down.ncf

Anstelle des alten Down Befehls (clib.nlm Files), sollte der Forcedown Befehl benutzt werden.

Mehrfacher Start von RCCMD auf Novell

Der Multi-Start von RCCMD auf Novell ist relativ einfach zu handhaben. Mehrere RCCMD Clients sollten mit folgendem Befehl gestartet werden:

load rccmd.nlm -l -a load down.ncf

Die Syntax lautet wie folgt:

LOADING RCCMD.NLM -L(Lauscher) -A(IP-Adresse des UPSMAN/CS121/RCCMD Senders) COMMAND (Auszuführender Befehl)

Beispiel:

LOAD RCCMD.NLM -L -A 192.168.10.2 LOAD DOWN.NCF

In diesem Szenario soll das “down.ncf” File ausgeführt werden, das zu einem sofortigen Shutdown des Client Computers führt, wenn das RCCMD Signal vom RCCMD Sender empfangen wurde.

Eine Gruppe von 8.ncf Files können Sie in dem UPSMAN Installations Verzeichnis finden. Bitte beachten Sie, dass diese Beispiel-Files vielleicht vom Benutzer/Administrator an die Konfiguration angepasst werden müssen.

5. RCCMD auf UNIX (mit grafischer Oberfläche)

Das RCCMD (Remote Console Command) ist ein Programm, das die Ausführung von Programmen auf Remote Computer ermöglicht. Dieses Tool ist Teil von allen UPSMAN unterstützten Betriebssystemen sowie aller GENEREX CS121 SNMP Manager, BACS WEBMANAGER oder RCCMD lizensierten SNMP Managern anderer Hersteller (z. B. RITTAL CMC, GENERAL ELECTRIC SNMP, CHLORIDE-MASTERGAURD usw.).

Das RCCMD Tool basiert auf dem TCP/IP Protokoll und arbeitet in zwei verschiedenen Modi. Das Modul arbeitet wie ein normales Programm, im Sender Modus, um RCCMD Befehle zu anderen Workstations zu senden, im Lauscher Modus, der als UNIX Daemon im Hintergrund läuft und auf Befehle wartet.

ACHTUNG:Wenn der Installer auf *einem 64bit Debian/Ubuntu (GNU/Linux)* nicht einwandfrei funktioniert, müssen die Kompatibilitäts-Libraries mit folgenden Befehl installiert werden: `sudo aptitude install ia32-libs`

INSTALLATION

RCCMD muss als user root von einer rootshell oder grafischen Terminal installiert werden. Dazu extrahieren Sie die Datei **rccmd.tar**, kopieren Sie nach z. B. */temp*, dann Start des Programms **rccmd.bin**. Es startet die folgende, grafische Installation:

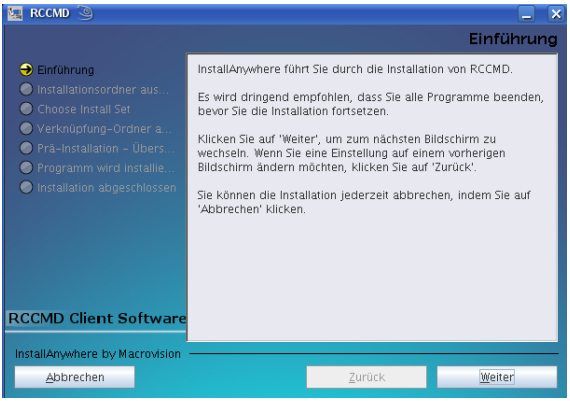

RCCMD
Einführung
Einführung
Installationsordner aus...
Choose Install Set
Verknüpfung-Ordner a...
Prä-Installation - Übers...
Programm wird installie...
Installation abgeschlossen
InstallAnywhere führt Sie durch die Installation von RCCMD.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die Installation fortsetzen.
Klicken Sie auf 'Weiter', um zum nächsten Bildschirm zu wechseln. Wenn Sie eine Einstellung auf einem vorherigen Bildschirm ändern möchten, klicken Sie auf 'Zurück'.
Sie können die Installation jederzeit abbrechen, indem Sie auf 'Abbrechen' klicken.
RCCMD Client Software
InstallAnywhere by Macrovision
Abbrechen
Zurück
Weiter

Abb. 51: Installation – Einführung

Es folgt die Eingabe des Lizenzschlüssels.

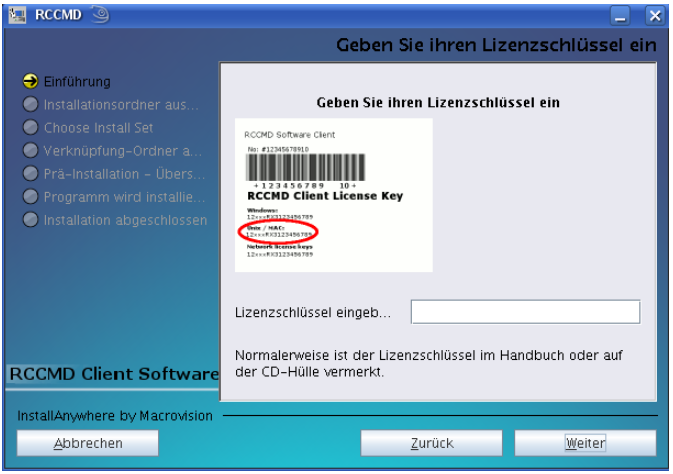


Abb. 52: Installation – Lizenzeingabe

Wählen Sie den gewünschten Installations-Pfad.

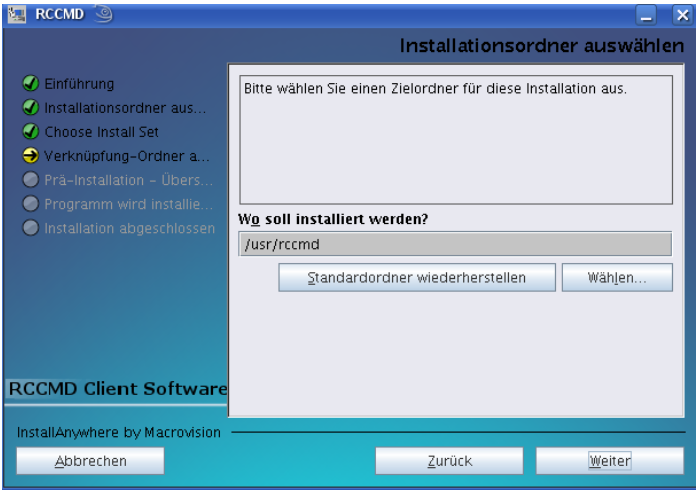


Abb. 53: Installation – Ordnerauswahl

Im nächsten Fenster können Sie die Options-Auswahl für die RCCMD Nachrichten treffen.

Abb. 54: Installation – Auswahl der Wiedergabemöglichkeiten

Es folgt die Zusammenfassung der Installation.

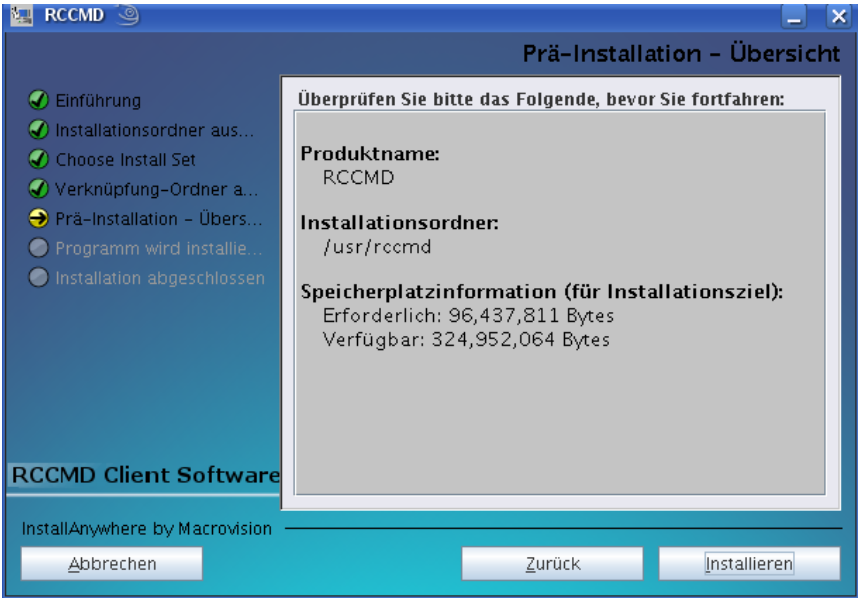


Abb. 55: Installation – Prä-Installations-Übersicht

Fügen Sie die IP-Adresse des RCCMD Servers hinzu, der authorisiert ist, ein Shutdown Signal zu diesem Client zu senden.

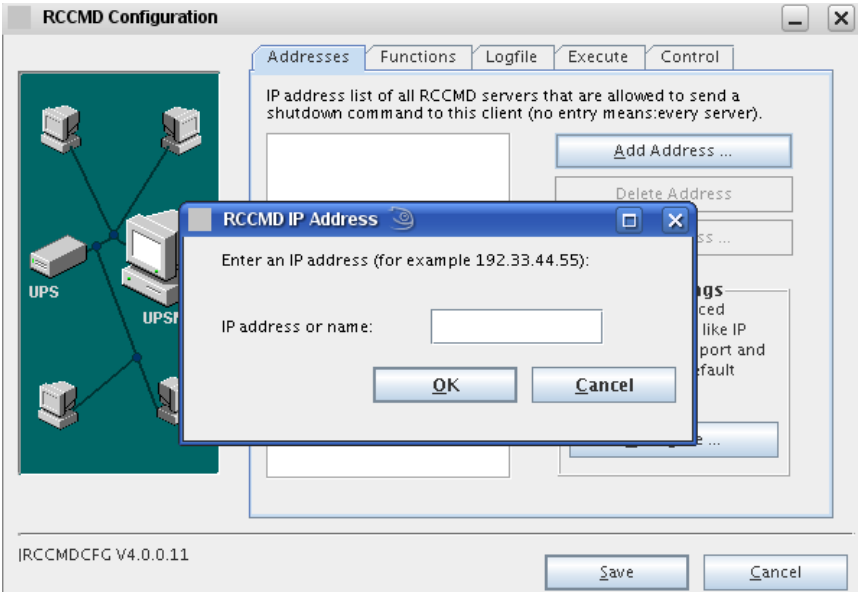


Abb. 56: Konfiguration – IP-Adressen Fenster

Achtung:

Wenn Sie keine Adresse eintragen, ist automatisch jeder Server authorisiert, ein Shutdown Signal zu senden. Wenn mehr als ein CS121 oder UPSMAN im Netzwerk existieren, also eine Redundanz Situation, müssen Sie mehrere Adressen als authorisierte Sender eintragen.

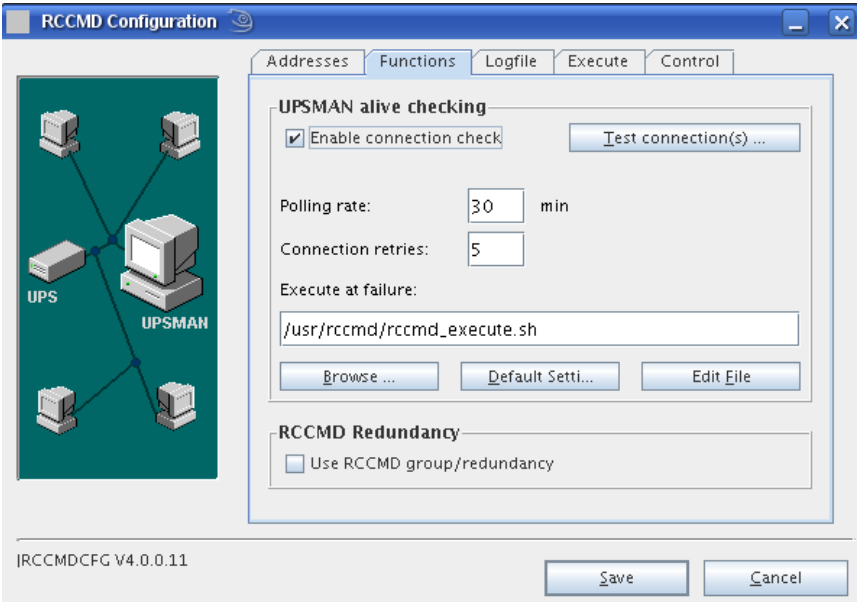


Abb. 57: Konfiguration – Functions

Wenn Sie die Funktion “UPSMAN Alive Checking” nutzen möchten (empfohlen), haken Sie die entsprechende Box an. Dieser Check ist ein Signal, dass an den CS121 oder UPSMAN via Port 5679 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “rccmd_execute.sh” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt. Die *Polling Rate* (Standard 30 Minuten) definiert den Interval der UPSMAN Abfrage, *connect retries* (Verbindungswiederholungen, Standard 5) bedeutet, das nach 5 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

Die Funktion “Use RCCMD Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigt. Wenn aktiviert, wird diese Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Wenn Sie auf “Test connections…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5679 wird getestet).

Wenn Sie auf “Browse…” klicken, werden Sie eine Auswahl der Standard SH-Files erhalten.

Wenn Sie auf „Default Setting“ klicken, werden Sie zurück zum „rccmd_execute.sh“ File gelangen.

Bei einem Fehler von dem UPSMAN Alive Check können Sie eine auszuführende Datei konfigurieren oder das Standard File editieren.

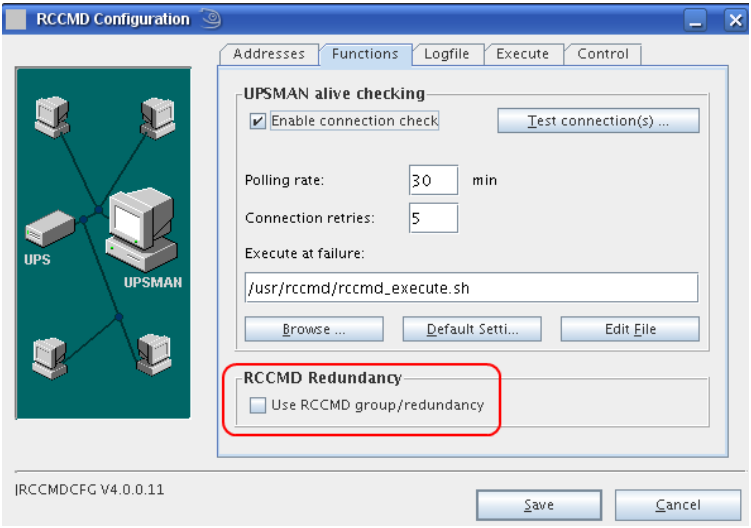


Abb. 58: Konfiguration – RCCMD Redundanz

Bei der USV Installation bietet RCCMD eine Redundanz Management Funktion wie folgt an:

Jede USV muss mit einem CS121 oder einem UPSMAN Software Computer ausgestattet sein. Wenn Sie die Box “Use RCCMD group/redundancy” anhaken, gelangen Sie zu einem Menü, welcher CS121/UPSMAN diesen RCCMD Client versorgt. Z.B.: Wenn 4 CS121/UPSMAN in 4 USVen installiert sind, dann kann jeder ein Shutdown Signal zu diesem RCCMD Client absetzen.

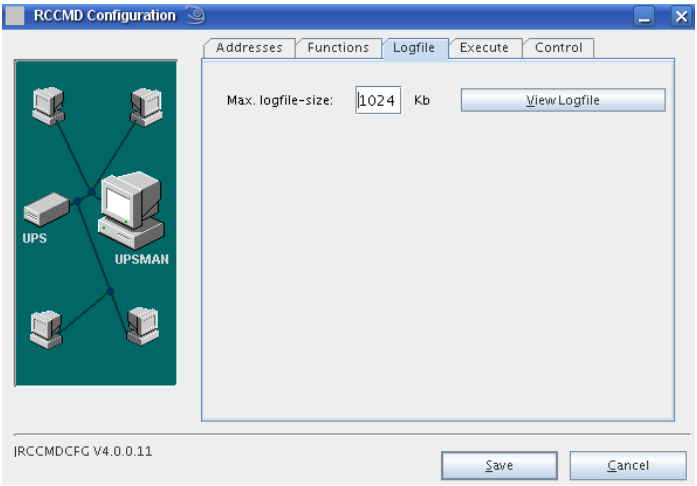


Abb. 59: Konfiguration – RCCMD Log File

Sie können die Log File Grösse konfigurieren und die auszuführenden Files editieren.

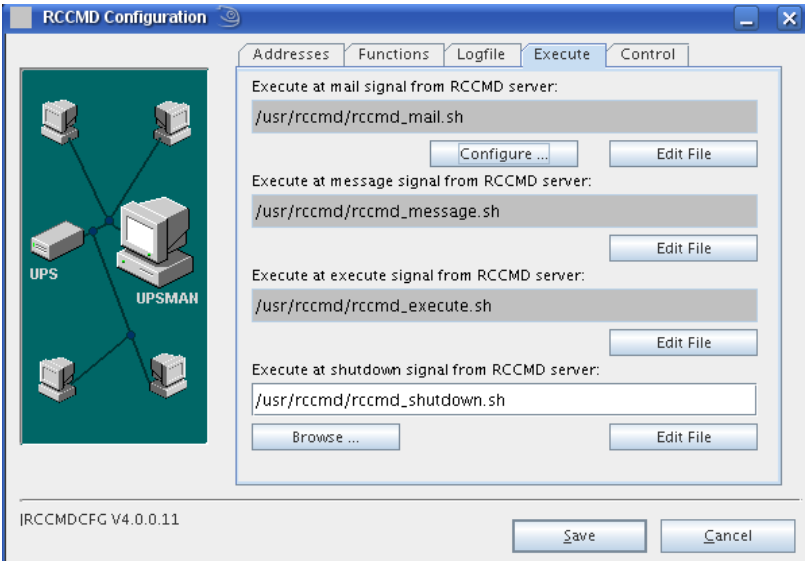


Abb. 60: Konfiguration – RCCMD Execute

Wenn Sie auf “Configure…” klicken, können Sie die Email Einstellungen vornehmen und die Mailfunktion von RCCMD nutzen.

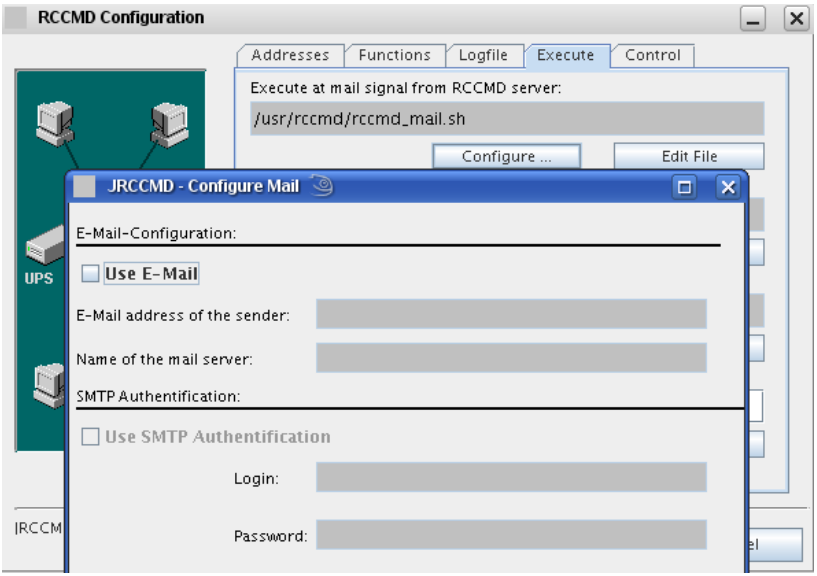


Abb. 61: Konfiguration – RCCMD Configure Email

Ab der RCCMD Version 4.0.2.0 gibt es auch eine grafische Konfiguration der Shutdown Sequenz.

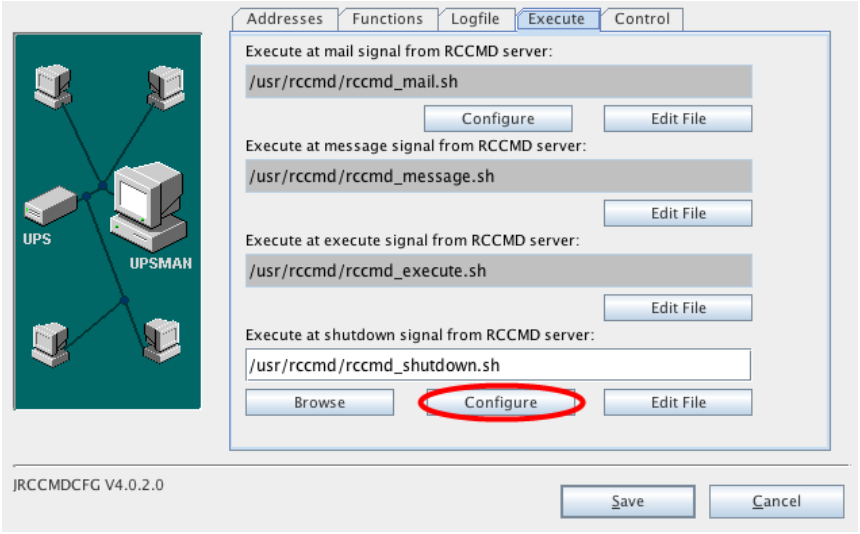


Abb. 62: Konfiguration – RCCMD Shutdown.sh

Klicken Sie auf „Configure“, um die Shutdown Sequenz zu öffnen.

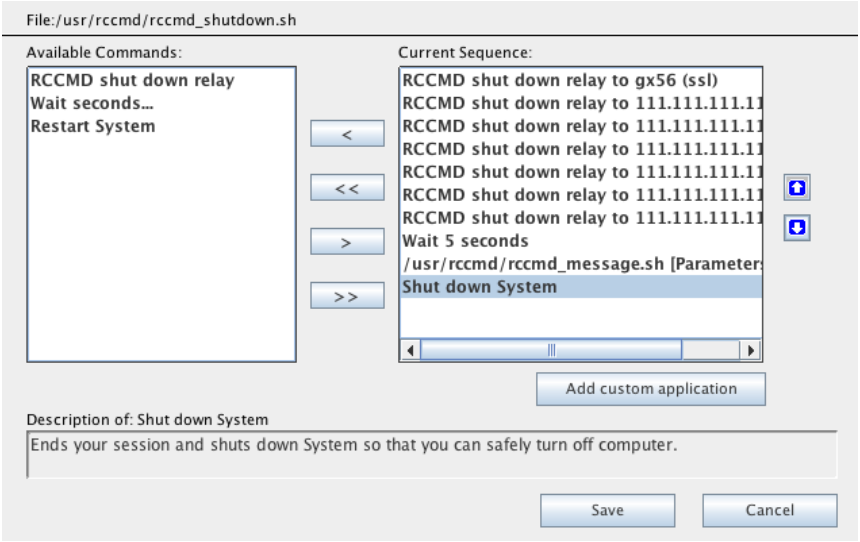


Abb. 63: Konfiguration – RCCMD Shutdown Sequenz

Die folgenden Befehle sind für die Shutdown Sequenz Konfiguration erhältlich:

RCCMD shutdown relay: Leitet einen RCCMD Shutdown Befehl an eine andere Workstation weiter (siehe auch Kapitel 5.4, Seite 75).

Wait seconds...: Warten eines Zeitraums in Sekunden, bis das nächste Kommando ausgeführt wird.

Restart System: Beendet Ihre Sitzung, fährt das System herunter und startet es neu.

Shutdown System: Beendet Ihre Sitzung und fährt das System herunter, sodass Sie sicher die Stromzufuhr unterbrechen können.

Über den „Control“ Button gelangen Sie zu der folgenden Maske:

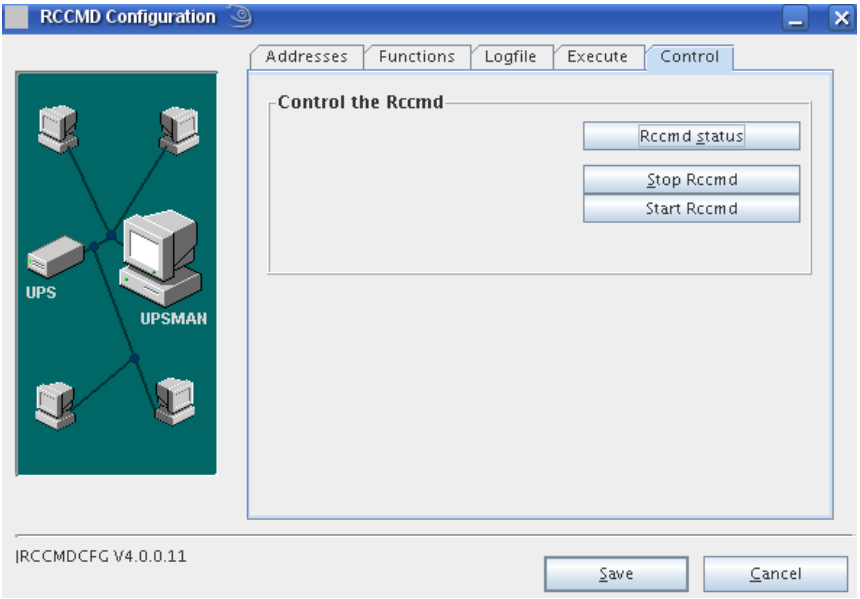


Abb. 64: Konfiguration – RCCMD Control

5.1 RCCMD mit Redundanz (ab RCCMD V3)

Redundanz ist die Vervielfachung von kritischen Komponenten von einem System mit der Absicht, die Ausfallsicherheit zu maximieren. In den meisten sicherheitskritischen Systemen sind einige Teile der Kontrolleinheit verdreifacht. Ein Ausfall von einer Komponente würde von den anderen beiden kompensiert werden. Bei einer Dreier-Redundanz verfügt das System über drei Sub-Komponenten, die alle fehlerhaft sein müssten, bevor das System ausfällt. Die Wahrscheinlichkeit, dass drei Komponenten gleichzeitig ausfallen, ist ziemlich gering.

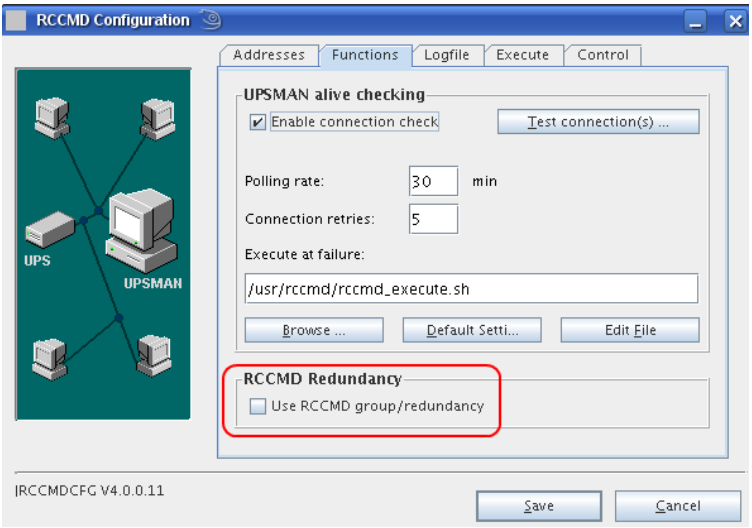


Abb. 65: Konfiguration – RCCMD mit Redundanz

Bei der USV Installation bietet RCCMD eine Redundanz Management Funktion wie folgt an:

Jede USV muss mit einem CS121 oder einem UPSMAN Software Computer ausgestattet sein. Wenn Sie die Box “Use RCCMD group/redundancy” anhaken, gelangen Sie zu einem Menü, welcher CS121/UPSMAN diesen RCCMD Client versorgt. Z.B.: Wenn 4 CS121/UPSMAN in 4 USVen installiert sind, dann kann jeder ein Shutdown Signal zu diesem RCCMD Client absetzen.

5.2 Silent Installation für die RCCMD Installation

Eine „Silent Installation“ ist eine automatisierte Installations-Prozedur, wo die Benutzerdaten von einem File empfangen werden. Dies ermöglicht die Software Installation ohne Eingaben vom Anwender oder einer grafischen Schnittstelle.

In der RCCMD Software besteht die Möglichkeit, eine Silent Installation (Automatisiert Hintergrundinstallation ohne Benutzerinput) zu aktivieren. Bevor man diese Funktion nutzen möchte, sind Einstellungen in der Datei „installer.properties“ notwendig. Diese befindet sich auf der UPS Management CD im Verzeichnis \Rccmd\Linux\12.

```
## This file provides Values to alter the behaviour of the installer.
## You can preset Values for some internal Variables.
## For the installer to find and use this file it is necessary to either rename
##  this file or pass a parameter to the installer when calling it.
##
## If this file is called 'installer.properties' or has the same name as the
##  installer, e.g. 'install_RCCMD.properties' then the installer should
##  automatically use this file.
##
## To call the installer with a parameter providing a properties file, the
##  installer need the parameter '-f' in this case the command line call looks
##  somewhat like this: "install_RCCMD.exe -f silent-installer.properties".
##
## To set the installer User Interface without providing the variable in the
##  properties file, the parameter '-i' can be used.
##  E.g. "install_RCCMD.exe -i silent"
##  The interface options are "silent,gui,console" the gui option is default.

## This will set the User Interface of the installer
#INSTALLER_UI=silent

## This presets the Licensekey. This value is necessary for a silent
##  installation, because there is no other way to pass this information to
##  the installer.
#GXLICENSEKEY=

## The Dialogbutton variable contains the answer to the pop-up questions whether
##  the RCCMD should be started at system boot and wether it should be started now.
##  the value '0' resembles the answer 'Yes' the value '1' (default) corresponds
##  to 'no'.
#CHOSEN_DIALOG_BUTTON=0

## Select the language for the installed version of RCCMD by setting the
##  INST_LANG variable to the desired country-code
##  (e.g.: el,en,es,de,fr,he,it,ja,ko,pt,ru,tr,zh_cn).
#INST_LANG=en
```

Abb. 66: Dateiinhalt „installer.properties“

Um die Silent Installation zu aktivieren, müssen Sie das Doppelkreuz vor der Variabel `INSTALLER_UI=silent` entfernen. Zusätzlich ist die Eingabe eines Lizenzschlüssels hinter der Variabel `GXLICENSEKEY=` erforderlich. Führen Sie die „installRCCMD.bin“ als root aus.

Weitere Optionen sind: `INSTALLER_UI=console` für die interaktive Installation ohne grafische Schnittstelle oder `INSTALLER_UI=console`, um die grafische Installation zu nutzen (Standard).

5.3 Console Installation für die RCCMD Installation

Eine Konsolen-Installation ist notwendig, wenn Ihr Zielsystem keine grafische Oberfläche für die Ausführung des „installRCCMD.bin“ besitzt. Diese Konsolen-Installation arbeitet interaktiv und wird die im „installer.properties“ siehe Abb. 64) aufgeführten Fragen auf der Konsole ausgeben, die der Benutzer beantworten muss.

Hinweis: Dies betrifft nur die Installation, die Konfiguration wird mittels Editor in der Datei „rccmd.cfg“ ausgeführt.

Um die Console Installation zu aktivieren, müssen Sie das Doppelkreuz vor der Variabel `INSTALLER_UI=` entfernen und `console` eintragen. Dies ist die interaktive RCCMD Installation auf der Konsole. Führen Sie als *root* die „installRCCMD.bin“ aus.

Mit der Variabel `CHOSEN_DIALOG_BUTTON=0`können Sie die Antwort auf die Frage definieren, ob der UPSMAN Dienst nach dem Systemstart automatisch gestartet werden soll. „0“ bedeutet ja, „1“ bedeutet nein.

Die Sprachauswahl können Sie mit der Variabel INST_LANG=de treffen, damit Ihnen bei der Konfiguration von der RCCMD Software die Tooltipps in der gewünschten Sprache zur Verfügung stehen.

Konfiguration der rccmd.cfg Datei in einer nicht grafischen Umgebung

Die Konfiguration von RCCMD muss per Editor erfolgen, wenn Sie keine grafische Schnittstelle haben. Die Konfigurationsdatei ist „rccmd.cfg“ und liegt im Standard RCCMD Verzeichnis (/usr/rccmd). Die Datei enthält im Kommentar die Beschreibung der einzelnen Konfigurationspunkte. Nachfolgend ein Beispielauszug aus der „rccmd.cfg“. Ändern Sie die Eingaben entsprechend Ihrer Installation:

```
########################################
# RCCMD Configuration
########################################
# Bind on Interface
# Defines on which interface we listen for incoming commands
# Default: 0.0.0.0 (All possible interfaces on this host)
ListenAddress=0.0.0.0
# Listen on Port
# Defines on which interface port we listen for incoming commands.
# Default: 6003
ListenPort=6003
```

```
# Enable UDP

# Defines if we should listen for rccmd (UDP) broadcasts

# Default: true

ListenUDP=true

# Access Control List

# A list of valid sender addresses, only its members can connect to us.

# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".

# Default: <empty> (Everyone is allowed to connect to us)

AllowedAddresses=

# Alive Check

# Enable Alive Check

# Defines if we should perform UPSMan alive checking.

# Default: false

AliveEnabled=false

# Alive Check Rate

# Defines the interval of UPSMan alive checking, in seconds.

# Default: 1800

AliveInterval=1800

# Alive Retry Rate

# Defines the number of UPSMan alive checking retries, in case of problems.

# Default: 0

AliveRetries=5

# Alive Check Group Members List

# A list of UPS device addresses that should be checked periodically.

# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".

# Default: <empty> (No alive checking)

AliveAddresses=

# Alive Program

# Full path to script that is executed when an alive check fails.
```

```
# Default: rccmd_notalive.sh

AliveProg=

# Redundancy Mode

# Enable Redundancy

# Defines if we should operate in redundancy mode.

# Requires an enabled <Alive Check> configuration.

# Default: false

RedundancyEnabled=false

# Redundancy Group Members List

# A list of redundancy group member addresses, must be also in <AliveAddresses>.

# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".

# Default: <empty> (No redundancy available)

RedundancyAddresses=

# Redundancy Level

# Defines how many of the <RedundancyAddresses> are redundant.

# Shutdown is executed when the number of shutdown requests exceeds this number.

# Default: 0 (No redundancy available)

RedundancyLevel=0

# Enable Redundancy Script

# Defines if we should NOT execute a script when redundancy suppresses a shutdown.

# Default: false.

RedundancyBatchSuppress=false

# Redundancy Script

# Full path to script that is executed when redundancy suppresses a shutdown.

# Default: ShutdownSuppressed.sh

RedundancyBatchFile=
```

Wenn Sie keine Einträge in der Standard „rccmd.cfg“ Datei verändern, werden alle eingehenen RCCMD Kommandos von jedem Sender ausgeführt und das Standard Shutdown-Skript „rccmd_shutdown.sh“ wird verwendet.

5.4 UNIX RCCMD Konfiguration mit CURSES Library

Hinweis: **Dieses Kapitel gilt für den Lauscher-Modus.**

RCCMD V2 im Lauscher Modus sollte mit Hilfe eines Konfigurations File konfiguriert werden. Standardmässig sucht RCCMD ein File mit dem Namen rccmd.cfg in seinem Startverzeichnis (/usr/ups). Dieses File sollte mit rccmd_conf. generiert werden. Rccmd_conf. Ist ein kleines Cursor basiertes Tool, welches auf einer Konsole, einem Terminal oder einer Terminal-Emulation unter X Windows System (z.B.: xterm) läuft.

Note: **Die Inhalte von rccmd.cfg sind grundlegend für die System Security. Nur der Sytem User "Root" sollte über Schreibrechte verfügen. Das Tool „rccmd_conf" wird von neueren Betriebssystemen nicht unterstützt. Wenn Sie versuchen, das Tool auf einem nicht unterstützten Betriebssystem auszuführen, erhalten Sie die Fehlermeldung über die nicht vorhandene „curses" library.**

Run rccmd_conf:

$ su -

Password:

cd /usr/ups

./rccmd_conf

Wenn rccmd.cfg nicht existiert (z.B.: wenn Sie rccmd_conf das erste Mal starten), erscheint folgende Meldung:

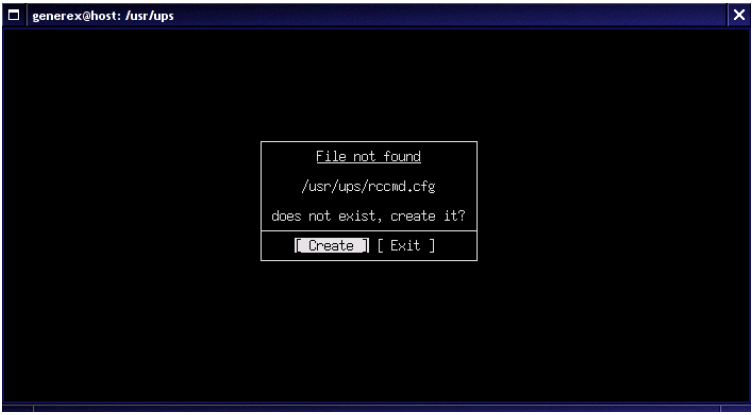


Abb. 67: Erstellung des Konfigurations-Files

Zum Fortfahren drücken Sie [Tab] solange [Create] markiert ist. Dann drücken Sie [Enter] oder wählen [Exit].

Wenn das File rccmd.cfg bereits existiert, wird rccmd_conf zu seinem Hauptkonfigurations-Menü wechseln.

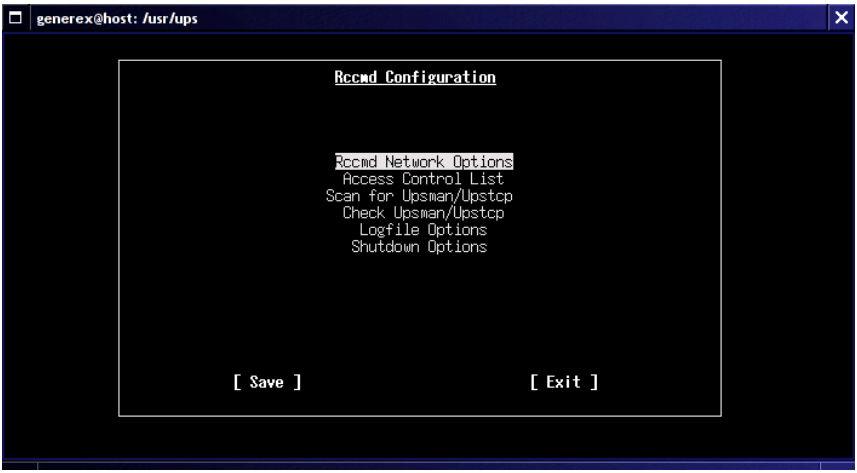


Abb. 68: RCCMD Konfigurations-Menü UNIX

Um zwischen den Menüeinträgen zu wechseln, drücken Sie [Tab] und/oder die Pfeiltasten. Um einen Eintrag auszuwählen, drücken Sie [Enter].

Es ist nicht erforderlich, von oben nach unten zu arbeiten. Sie können die Menüpunkte in beliebiger Reihenfolge konfigurieren. Wenn Sie nichts konfigurieren, werden die Standardwerte verwendet, wenn Sie auf [Save] drücken. Wir empfehlen, RCCMD (rccmd.cfg) individuell zu konfigurieren, um alle Features nutzen zu können und um die Sicherheit zu erhöhen.

Konfiguration der “RCCMD Network Options”

In diesem Fenster können Sie die Netzwerk relevanten Optionen von dem RCCMD Lauscher konfigurieren. Um zwischen den Options-Feldern zu wechseln, nutzen Sie die [Tab] Taste.

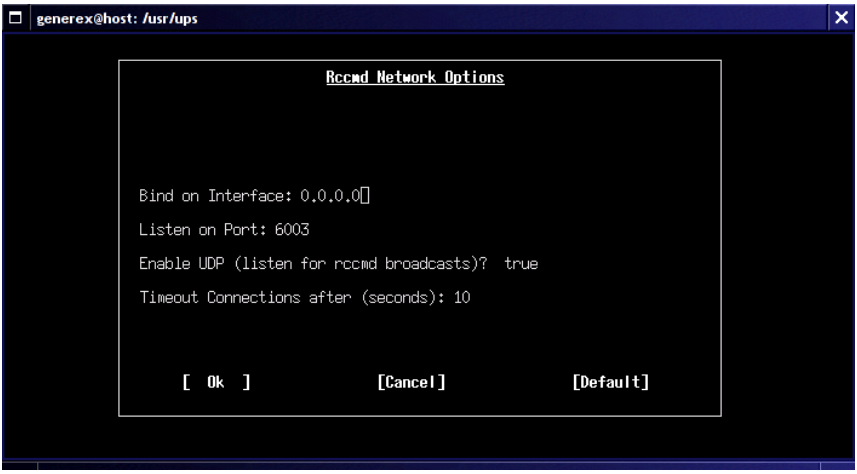


Abb. 69: RCCMD UNIX Netzwerk Optionen

Schnittstellenanbindung:

Mit dieser Option wird definiert, welche Netzwerk-Schnittstelle an das Haupt TCP Lauscher *Socket* angebunden ist. Sie können jede gültige IP-Adresse angeben, auf die der Host erreicht werden kann.

Der Standardwert für diese Option ist 0.0.0.0, dies ist ein gültiger Wert, der bedeutet, dass auf alle möglichen Schnittstellen gelauscht wird. Wenn der Host eine Dial-Up-Verbindung zum Internet hat, sollten Sie den Standardwert verändern, um sicherzustellen, das RCCMD nicht vom Internet aus verbunden wird. In diesem Fall sollten Sie die IP-Adresse von dem Host eintragen, auf dem der RCCMD Lauscher läuft.

Beispiel:

Ihr Computer läuft in einem privaten Netzwerk in dem 192.168.1.0/24 Adressbereich. Der RCCMD Lauscher läuft auf der vergebenen IP-Adresse192.168.1.9. Sie sollten diese Adresse im Feld “Bind On Interface” eintragen, um sicherzustellen, dass nur Workstations aus dem privaten Netzwerk eine Verbindung zu RCCMD herstellen können.

Lauschen auf Port:	Dies ist der Port, auf dem RCCMD als Lauscher läuft. Der erlaubte Wertebereich liegt zwischen 1 und 65535 (inklusive). Der Standard-Port ist 6003. Wenn Sie den Port von dem RCCMD Lauscher verändern, müssen Sie auch den Port von dem RCCMD Sender verändern, um eine Verbindung herzustellen. Es ist eigentlich nicht notwendig, den Standard-Port zu verändern.
UDP Aktivierung:	Wenn diese Option aktiviert ist, wird RCCMD automatisch einen UDP Lauscher Socket anstelle des TCP Socket öffnen. Dies ermöglicht dem RCCMD Lauscher, RCCMD Broadcasts zu empfangen. Mögliche Werte sind “true” oder “false”, der Standard ist “true”.
Timeout:	Zeitüberschreitung für TCP Verbindungen. Der Standard ist 10 Sekunden. Es ist eigentlich nicht notwendig, diese Einstellung zu ändern.

Um alle Werte auf die Standardwerte zurückzusetzen, wählen Sie [Default] mit einem Klick auf [Tab] und drücken Sie [Enter].

Um die Maske zu verlassen, wählen Sie entweder [Ok] (Werte akzeptieren wie dargestellt) oder [Cancel] (alle Änderungen verwerfen).

Konfiguration der “Access Control List”

“Access Control List” beinhaltet eine Liste von gültigen Sender Adressen. Eine gültige Sender Adresse ist die IP-Adresse von einem RCCMD Sender, der berechtigt ist, eine Verbindung zu einem RCCMD Lauscher herzustellen.

Achtung: **Eine leere “Access Control List” bedeutet, dass jeder berechtigt ist, eine Verbindung herzustellen.**

Um zwischen den Einträgen in der Liste hin- und herzuwechseln, benutzen Sie die [↑] und [↓] Tasten. Um einen Eintrag auszuwählen, drücken Sie [Enter].

Abb. 70: Hinzufügen RCCMD UNIX Sender

Um eine IP-Adresse hinzuzufügen, drücken Sie [Tab], bis [Add] markiert ist, und drücken Sie [Enter].

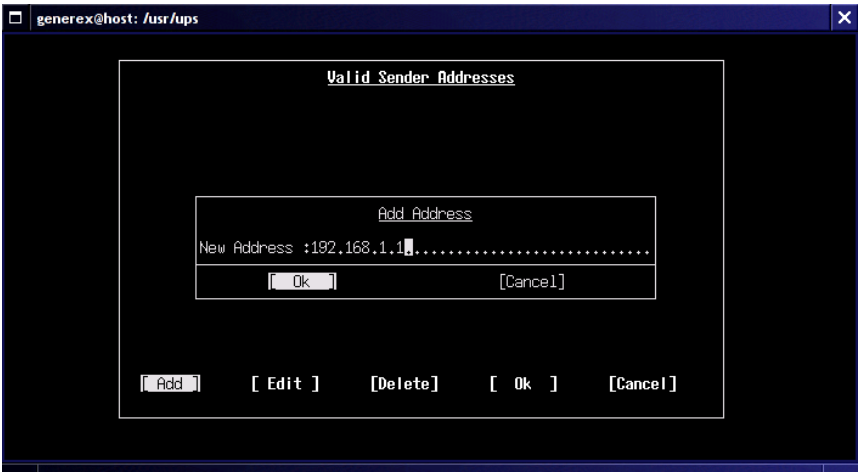


Abb. 71: RCCMD UNIX Sender Beispiel

Tragen Sie die IP-Adresse von der Workstation ein, die in der Lage sein soll, eine Verbindung herzustellen, dann drücken Sie [Enter].

Abb. 72: RCCMD UNIX Sender Überblick

Um einen Eintrag zu editieren, wählen Sie mit [↑] und [↓], bis der gewünschte Eintrag markiert ist. Danach drücken Sie [Tab] bis [Edit] markiert ist und drücken [Enter].

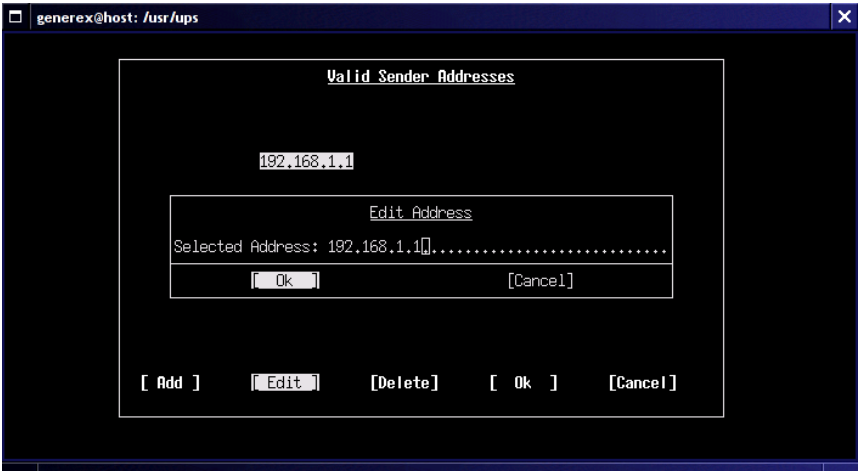


Abb. 73: RCCMD UNIX Sender Editierung

Sie können die Adresse im “Edit Address” Fenster editieren. Um Ihre Veränderungen zu speichern, wählen Sie [Ok] und drücken [Enter], andererseits [Cancel].

Um einen Eintrag in der Liste zu löschen, nutzen Sie die [↑] und [↓] Tasten, bis der gewünschte Eintrag markiert ist, drücken [Delete] und [Enter].

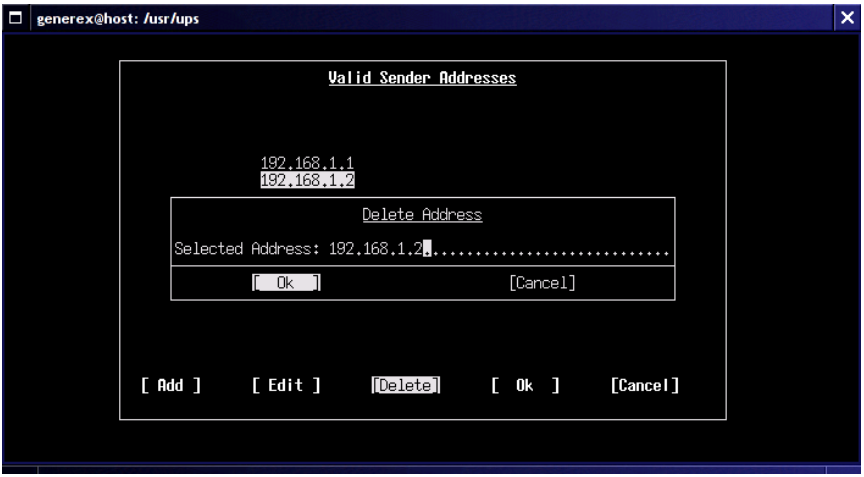


Abb. 74: RCCMD UNIX Sender Löschen

Bestätigen Sie das Löschen des Eintrags mit [Ok] und [Enter]. Um die Maske zu verlassen, wählen Sie entweder [Ok] (Werte akzeptieren wie dargestellt) oder [Cancel] (alle Änderungen verwerfen).

Netzwerkabfrage nach UPSMAN/UPSTCP:

Dieses Fenster bietet die Möglichkeit, das Netzwerk nach UPSMAN/UPSTCP Servern abzusuchen. Sie sollten die ermittelten IP-Adressen zu Ihrer “Access Contrtol List” hinzufügen.

Hinweis: **Die Optionen in diesen Fenstern beeinflussen RCCMD nicht direkt, aber die Ergebnisse der Netzwerkabfrage sollten in die “Access Control List” eingetragen werden.**

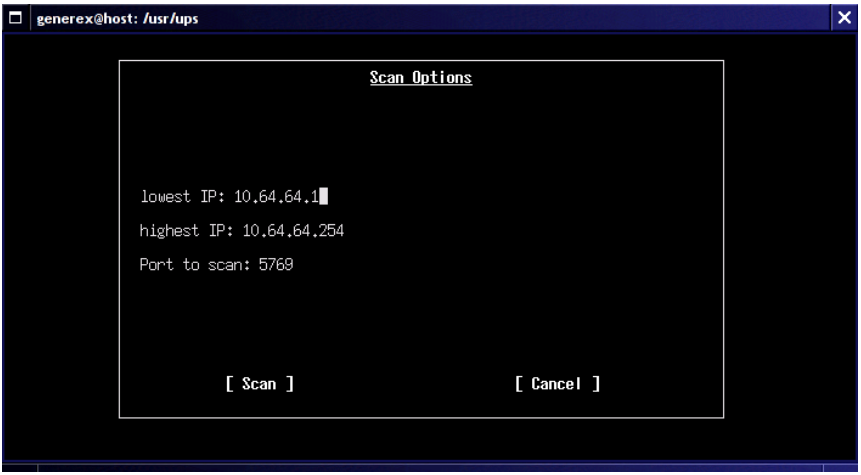


Abb. 75: RCCMD UNIX Sender Scan

lowest/highest IP:	Beim Start versucht die rccmd_conf, die primäre IP-Adresse des Hosts zu ermitteln. Von dieser Adresse wird ein korrespondierender Klasse C Netzwerkbereich abgeleitet. Dies sind die Standard Begrenzungen für eine Netzwerkabfrage. Wenn Sie ein anderes Netzwerk abfragen möchten oder den Bereich abstimmen möchten, verändern Sie in den “Scan Options” die Adressen (lowest and/or highest IP address).
Port to scan:	Der Port, zu dem sich der Scanner versucht zu verbinden. Der Standard Port ist 5769, gleichzeitig der Standard Port des UPSMAN/UPSTCP Servers. Wenn Sie den UPSMAN/UPSTCP auf einem anderen Port laufen haben, sollten Sie den Standard Port zur Abfrage dementsprechend ändern.

Um die Abfrage zu starten, wählen Sie [Scan] und drücken [Enter], andererseits [Cancel].

Konfiguration “Check Upsman/Upstcp”:

Der RCCMD Lauscher hat die Fähigkeit, den “Alive Check” zum UPSMAN/UPSTCP Servers periodisch durchzuführen.

Hinweis: **Das “Check UPSMAN/UPSTCP Feature ist nur verfügbar, wenn Sie mindestens eine Adresse in der “Access Control List” eingetragen haben.**

Wenn Sie mehrere Adressen in der Liste eingetragen haben, erscheint folgendes Pop-Up-Fenster:

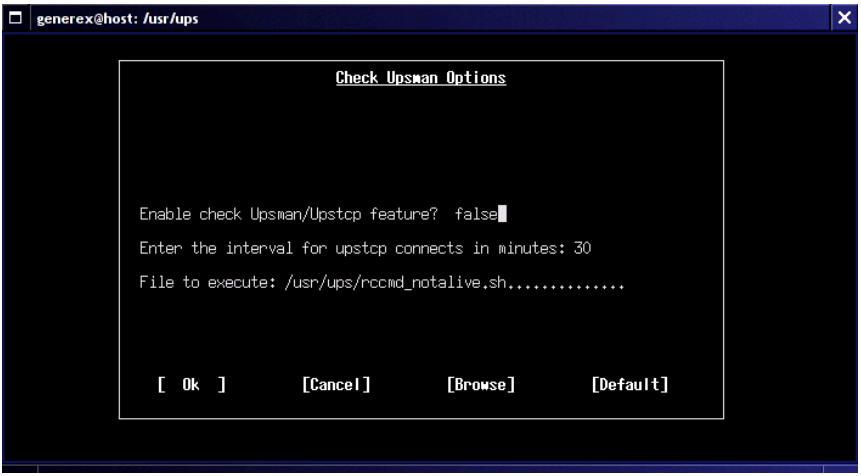


Abb. 76: RCCMD UNIX Check Upsman

Benutzen Sie [Tab], um sich zwischen den Options-Feldern und Buttons zu bewegen.

Enable check Upsman/Upstcp feature: Mögliche Werte sind “true” oder “false”, “false” ist Standard. Um den Wert zu verändern, nutzen Sie [↑] und [↓].

Enter the interval for upstcp connects in minutes:

Intervall-Angabe in Minuten. Der Standard ist 30 Minuten. Um diesen Wert zu verändern, überschreiben Sie den Wert im Options-Feld.

File to execute: Dieses File wird ausgeführt, wenn RCCMD nicht in der Lage ist, eine Verbindung zu einem oder mehreren UPSMAN/UPSTCP Servern herzustellen, in der Annahme, das entweder der HOST unten ist oder der UPSMAN/UPSTCP Dienst nicht läuft. Standard ist “/usr/ups/rccmd_notalive.sh”. Wenn Sie diesen Wert verändern möchten, überschreiben Sie den String im Optionen-Feld oder mit der Auswahl eines Files. Um den File-Browser zu aktivieren,

drücken Sie [Tab] bis [Browse] markiert ist und drücken [Enter].

Um alle Werte auf die Standardwerte zurückzusetzen, wählen Sie [Default] mit einem Klick auf [Tab] und drücken Sie [Enter].

Um die Maske zu verlassen, wählen Sie entweder [Ok] (Werte akzeptieren wie dargestellt) oder [Cancel] (alle Änderungen verwerfen).

Konfiguration der “Logfile Options”:

Der RCCMD Lauscher ist in der Lage, ein Log File zu schreiben und es zu pflegen/warten. Es loggt Events wie Start/Stopp des Programms, akzeptierte und abgelehnte Netzwerk Verbindungen und ausgeführte Befehle/Files. Einige Parameter können Sie in den Log File Optionen eintragen:

Abb. 77: RCCMD UNIX Log File Optionen

Enable logging to file:	Mögliche Werte sind “true” oder “false”, “false” ist Standard. Um den Wert zu verändern, nutzen Sie [↑] und [↓].
Select maximum size of log file:	Das Log File wird nicht größer sein als dieser Wert. Wenn es dieses Limit überschreiten würde, würde RCCMD es erst um 10% verkleinern, um dann mit dem Loggen fortzufahren. Das Log File wird vom Start verkleinert, sodass ältere Einträge zuerst gelöscht werden würden. Die Standard Größe ist 1024 Kb. Um diesen Wert zu verändern, nutzen Sie [↑] und [↓]. Der Spezial-

	Wert “0” bedeutet, dass das File nicht verkleinert oder überschrieben werden würde.
Log file name:	Diese Option spezifiziert den Namen und dien Ort des Log Files. Der Standard ist “/usr/ups/rccmd.log”. Wenn Sie diesen Wert verändern möchten, überschreiben Sie den String im Optionen-Feld oder mit der Auswahl eines Files. Um den File-Browser zu aktivieren, drücken Sie [Tab] bis [Browse] markiert ist und drücken [Enter].

Um alle Werte auf die Standardwerte zurückzusetzen, wählen Sie [Default] mit einem Klick auf [Tab] und drücken Sie [Enter].

Um die Maske zu verlassen, wählen Sie entweder [Ok] (Werte akzeptieren wie dargestellt) oder [Cancel] (alle Änderungen verwerfen).

Konfiguration der “Shutdown Options”:

Abb. 78: RCCMD UNIX Shutdown Optionen

File to execute:	Dieses File wird ausgeführt, wenn RCCMD den “Shutdown” Befehl empfängt. Standard ist “/usr/ups/rccmd_shutdown.sh”

Um alle Werte auf die Standardwerte zurückzusetzen, wählen Sie [Default] mit einem Klick auf [Tab] und drücken Sie [Enter].

Um die Maske zu verlassen, wählen Sie entweder [Ok] (Werte akzeptieren wie dargestellt) oder [Cancel] (alle Änderungen verwerfen).

Beenden der rccmd_conf:

In der Hauptkonfiguration “RCCMD Configuration” wählen Sie entweder [Save] oder [Exit] und drücken [Enter]. Save bedeutet, dass rccmd.cfg wird mit seinen aktuellen Werten, die Sie auf dem Bildschirm sehen, gespeichert. Mit Exit verlassen Sie das Programm, ohne die rccmd.cfg berührt zu haben.

Der File Browser:

Einige der Konfigurations-Masken nutzen einen integrierten File Browser:

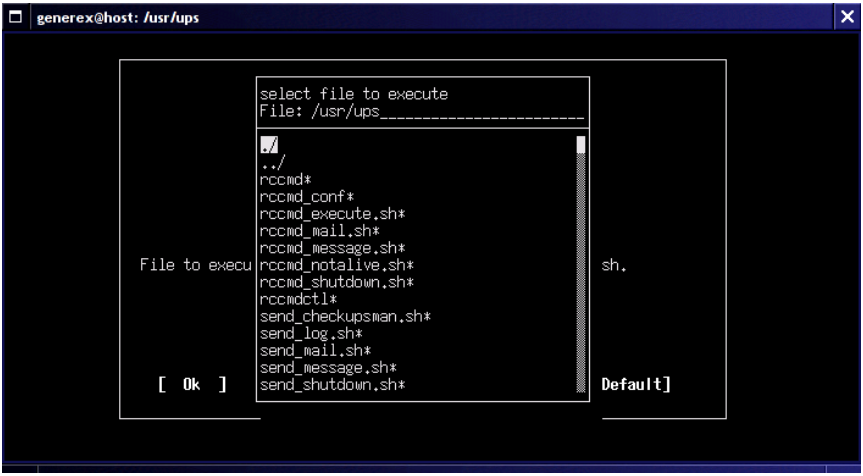


Abb. 79: RCCMD UNIX File Browsing

Die [↑] und [↓] Tasten können zum Bewegen in der Liste genutzt werden. Mit dem Drücken von [Enter] wählen Sie den markierten Eintrag aus. Wenn der ausgewählte Eintrag ein Verzeichnis ist, wird der Browser das Verzeichnis und seine Inhalte auflisten. Dateitypen können mit den Eingaben “ls-F” angezeigt werden. Sternchen “*” bedeuten auszuführende Dateien, Schrägstriche “/” für Verzeichnisse, “@” für symbolische Links und Gleichheitszeichen “=” für Sockets.

UNIX RCCMD multiple Sender Konfiguration :

Wenn Sie mehr als eine Sender-Adresse verwenden möchten, sollte die rccmd.sh wie folgt modifiziert werden:

```
#! /bin/sh

# You may specify a sender IP to accept signals from,
# default is everyone.
SENDER="-a 10.55.52.82 -a 10.55.52.83 -a 10.55.52.84"

# You may change the port to listen on,
```

```
# default is 6003.
PORT=

# You must define a command to be executed upon
# receiving signal.
SCRIPT=/usr/ups/doshutdown.sh

# test -z $SENDER || SENDER="-a $SENDER"
test -z $PORT || PORT="-p $PORT"
# to start:
./rccmd -l $SENDER $PORT $SCRIPT
```

UNIX RCCMD multiple Sender Konfiguration (V3 und höher):

Wie starte ich den Rccmd V3 mehrfach über verschiedene Ports auf einer UNIX Maschine?
Dafür muss jedes RCCMD einen eigenen TCP-Port bekommen, z.B.:

```
./rccmd -l -p 6003
./rccmd -l -p 6004
./rccmd -l -p 6005
```

Import in die RC Files:

Am einfachsten wäre es, eine entsprechende Anzahl neuer Startskripte anzulegen und diese dann durch das alte aufzurufen, z.B.:

1) Neue Startskripte erzeugen:
Dazu altes Skript dreimal kopieren und dabei umbennenen:

```
cp rccmdctl.sh rccmdctl-1.sh
cp rccmdctl.sh rccmdctl-2.sh
cp rccmdctl.sh rccmdctl-3.sh
```

2) Neue Startskripte anpassen:
Dazu in jedem der drei neuen Skripte durch die Variable 'RCCMDPORT' den TCP-Port anpassen:

```
...
   RCCMDPORT=6003
...
```

3) Altes Startskript anpassen, damit dieses die neuen Skripte nachstartet.
Dazu mindestens den 'start' und den 'stop' -Zweig in der Datei 'rccmdctl' ersetzen:

```
  start)
     /usr/ups/rccmdctl-1.sh start
     /usr/ups/rccmdctl-2.sh start
     /usr/ups/rccmdctl-3.sh start
   ;;

   stop)
     /usr/ups/rccmdctl-1.sh stop
```

```
    /usr/ups/rccmdctl-2.sh stop
    /usr/ups/rccmdctl-3.sh stop
  ;;
```

ACHTUNG:

Diese Skripte NICHT mit einem Windows-Editor bearbeiten, dann werden diese wegen der unterschiedlichen Zeilenumbrüche auf Windows/Unix zerstört!

5.5 Der RCCMD Client als Relay Station

Wenn Sie eine grössere Anzahl von RCCMD Empfänger erreichen möchten, muss der CS121 Adapter als Relay Station fungieren. Der Empfänger wird so konfiguriert, dass er beim Erhalten eines RCCMD Signals eine Script startet, das weitere RCCMD Signale versendet. Diese Workstation ist dann Empfänger und Sender zur gleichen Zeit und somit eine wichtige Verbindung in der USV Überwachungskette. Der Gebrauch von einem RCCMD Client als Relay Station macht die Überwachung von mehreren hundert RCCMD Clients sehr viel einfacher als die Konfiguration über das Web-Interface des CS121. Außerdem haben alle Webbrowser Event Konfigurationen eine Sicherheits-Limitierung, sodas es erforderlich ist, diese Relay Funktion zu nutzen, wenn die Anzahl der Jobs 50 pro Event auf dem CS121 HW131 übersteigt.

So richtet man ein RCCMD Relay (Weiterleitung des Shutdown-Signals) ein:

- Öffnen Sie die Datei „rccmd_shutdown.sh“ mit einem Editor.
- Fügen Sie vor dem Shutdown des Computers (in der Zeile „shutdown –h now“) die Relay Aufrufe ein, z.B. einen Aufruf des mitgelieferten Scriptes „send_shutdown.sh“.
- Diesem Script können gleich mehrere IP-Adressen oder DNS-Namen der gewünschten Relay Empfänger übergeben werden, z.B:

```
./send_shutdown.sh -a 10.10.10.10 -a 10.10.10.11 -a 10.10.10.12
```

- Speichern Sie die Änderungen der Datei „rccmd_shutdown.sh“.

Ab der RCCMD Version 4.0.2.0 gibt es auch eine grafische Konfiguration der Shutdown Sequenz.

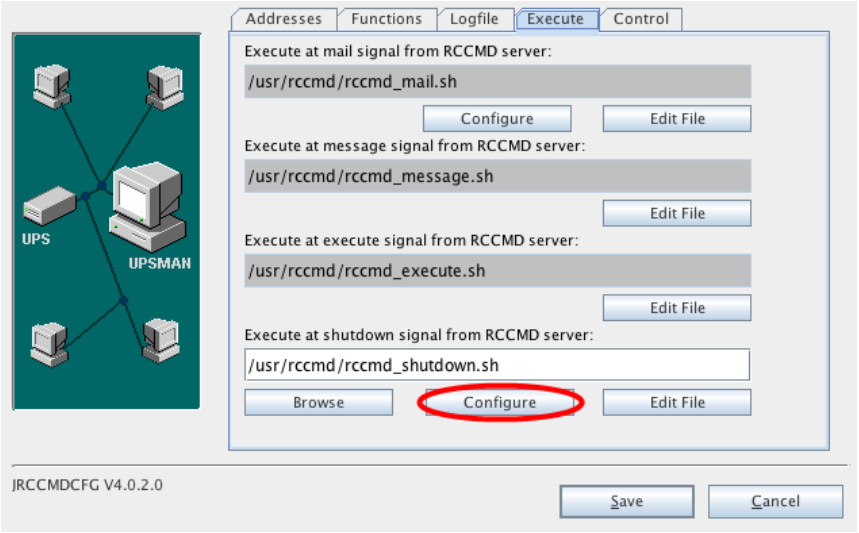


Abb. 80: Konfiguration – RCCMD Shutdown.sh

Klicken Sie auf „Configure“, um die Shutdown Sequenz zu öffnen.

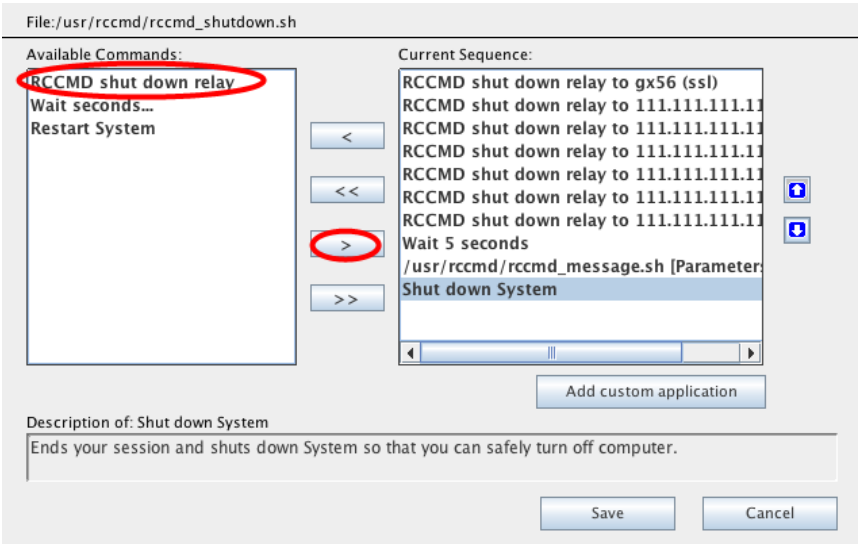


Abb. 81: Konfiguration – RCCMD Shutdown Sequenz

Wenn Sie „RCCMD shut down relay markiert haben und den Pfeil „>“ klicken, öffnet sich folgendes Fenster, in dem man den gewünschten IP-Adressen-Bereich eingeben kann oder eine einzelne IP-Adresse bzw. Hostnamen.

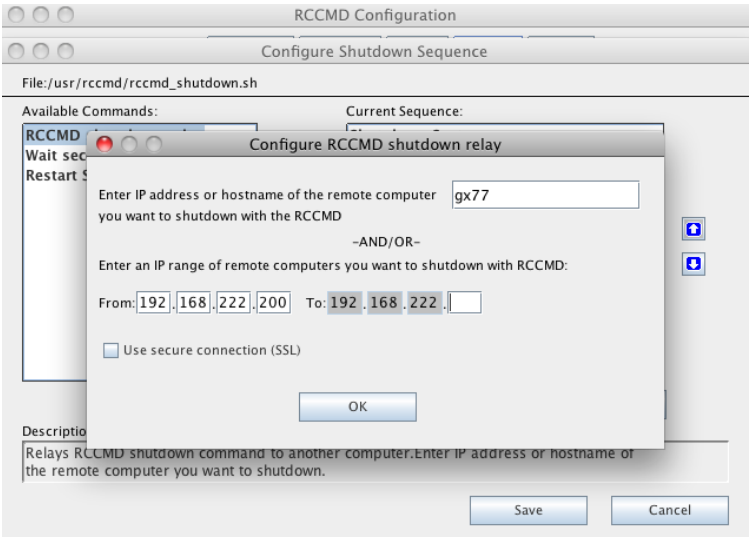

RCCMD Configuration
Configure Shutdown Sequence
File:/usr/rccmd/rccmd_shutdown.sh
Available Commands:
Current Sequence:
Configure RCCMD shutdown relay
Enter IP address or hostname of the remote computer you want to shutdown with the RCCMD
gx77
-AND/OR-
Enter an IP range of remote computers you want to shutdown with RCCMD:
From: 192 . 168 . 222 . 200
To: 192 . 168 . 222 .
Use secure connection (SSL)
OK
Relays RCCMD shutdown command to another computer.Enter IP address or hostname of the remote computer you want to shutdown.
Save
Cancel

Abb. 82: Konfiguration – RCCMD Relay Konfiguration IP-Adressen-Bereich

Ausserdem kann man hier auch die SSL-Funktion aktivieren (siehe auch Kapitel 5.5).

Um einzelne IP-Adressen aus dem Bereich zu entfernen, markieren Sie die Zeile auf der rechten Seite mit der entsprechenden IP-Adresse, und klicken Sie auf den Pfeil „<“.

5.6 RCCMD mit SSL auf UNIX

Das *Secure Sockets Layer* (SSL) Protokoll ist ein kryptografisches Protokoll, das Sicherheit und Datenintegrität für Kommunikationen in TCP/IP Netzwerken bietet.

Stellen Sie über einen Webbrowser eine Verbindung zum CS121 SNMP Adapter her. Klicken Sie im Konfigurations-Menü auf “Network & Security”, und setzen Sie den Haken bei “Use RCCMD SSL”.

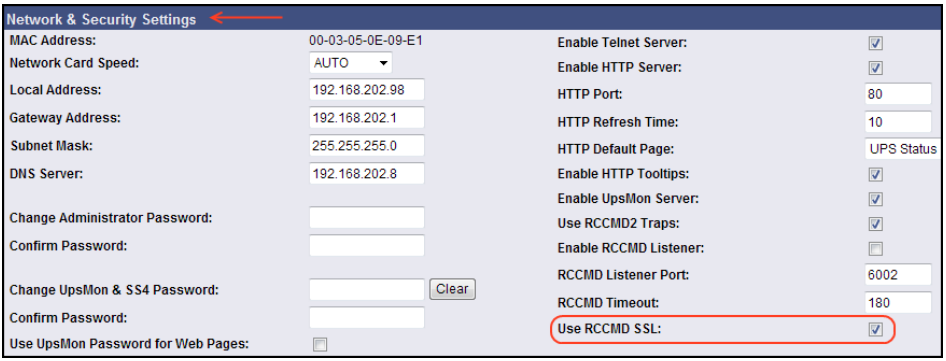


Abb. 83: RCCMD SSL Konfiguration

Das SSL Netzwerk Feature erfordert einen korrekten Zeitstempel. Konfigurieren Sie im „Timeserver“ Menü eine entsprechende IP-Adresse.

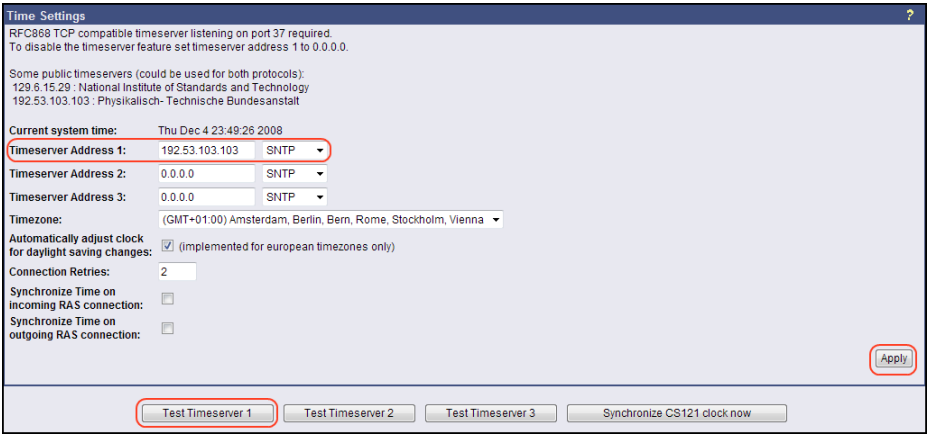

Time Settings
RFC868 TCP compatible timeserver listening on port 37 required.
To disable the timeserver feature set timeserver address 1 to 0.0.0.0.
Some public timeservers (could be used for both protocols):
129.6.15.29 : National Institute of Standards and Technology
192.53.103.103 : Physikalisch- Technische Bundesanstalt
Current system time: Thu Dec 4 23:49:26 2008
Timeserver Address 1: 192.53.103.103 SNTP
Timeserver Address 2: 0.0.0.0 SNTP
Timeserver Address 3: 0.0.0.0 SNTP
Timezone: (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Automatically adjust clock for daylight saving changes: (implemented for european timezones only)
Connection Retries: 2
Synchronize Time on incoming RAS connection:
Synchronize Time on outgoing RAS connection:
Apply
Test Timeserver 1
Test Timeserver 2
Test Timeserver 3
Synchronize CS121 clock now

Abb. 84: Timeserver Konfiguration

Klicken Sie auf das „Save Configuration“ Menü, und bestätigen Sie Ihre Einstellungen mit „Save, Exit & Reboot“.

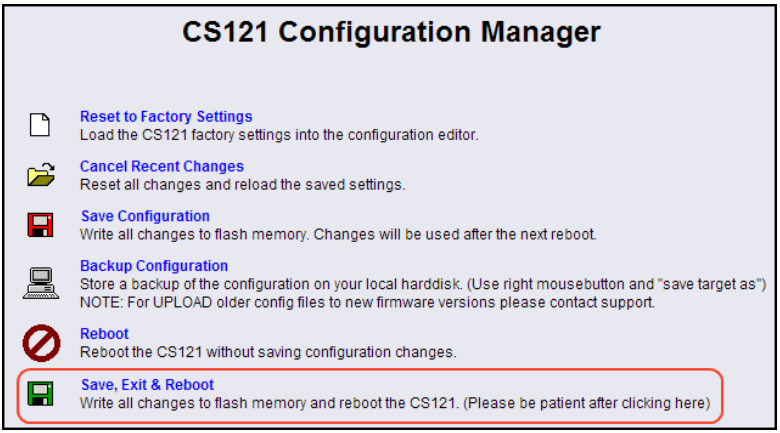

CS121 Configuration Manager
Reset to Factory Settings
Load the CS121 factory settings into the configuration editor.
Cancel Recent Changes
Reset all changes and reload the saved settings.
Save Configuration
Write all changes to flash memory. Changes will be used after the next reboot.
Backup Configuration
Store a backup of the configuration on your local harddisk. (Use right mousebutton and "save target as")
NOTE: For UPLOAD older config files to new firmware versions please contact support.
Reboot
Reboot the CS121 without saving configuration changes.
Save, Exit & Reboot
Write all changes to flash memory and reboot the CS121. (Please be patient after clicking here)

Abb. 85: Speichern der Einstellungen

Gehen Sie in das RCCMD Installations Verzeichnis (z. B. /usr/ups), und starten Sie die RCCMD Configuration:

```
/rccmdctl conf
```

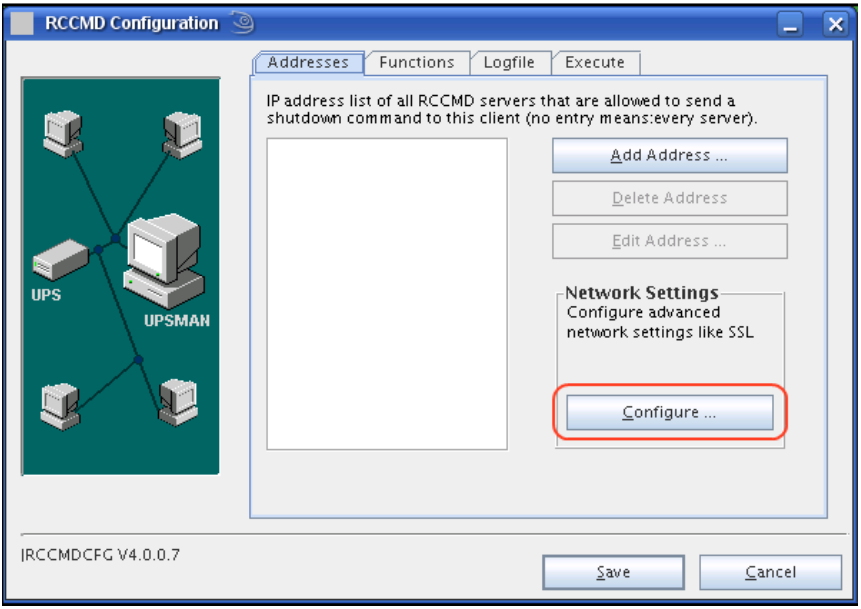


Abb. 86: SSL Konfiguration

Aktivieren Sie das SSL Netzwerk Feature.

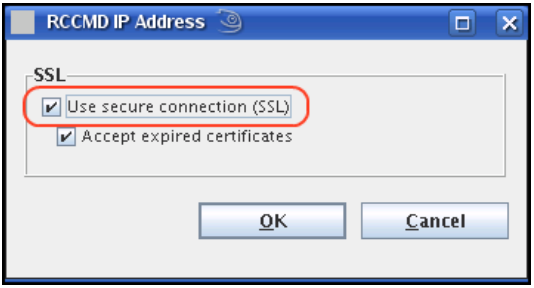


Abb. 87: Advanced Network Settings

Alternative Konfiguration mit einem Text-Editor

Sie können die gewünschte Konfiguration mit einem ASCII-Editor manuell in die Konfigurationsdatei „rccmd.cfg“ eintragen.

```
# RCCMD Configuration (v2-default)

#

# Bind on Interface

# Defines on which interface we listen for incoming commands

# Default: 0.0.0.0 (All possible interfaces on this host)
```

```
#
ListenAddress=0.0.0.0
#
# Listen on Port
# Defines on which interface port we listen for incoming commands.
# Default: 6003
#
ListenPort=6003
#
# Enable UDP
# Defines if we should listen for rccmd (UDP) broadcasts
# Default: true
#
ListenUDP=true
#
# Access Control List
# A list of valid sender addresses, only its members can connect
to us.
# Seperate IP addresses with a space, e.g.: "192.168.0.1
192.168.0.2".
# Default: <empty> (Everyone is allowed to connect to us)
#
AllowedAddresses=
#
# SSL: Use SSL
# Enables (true) or disables (false) SSL Connections
# Default: false
#
SSL=false
#
```

```
# SSL: Reject expired certificates

# Permits (false) or denies (true) connections with expired
cert's.

# Default: false

#

SSLRejectExpiredCert=false
```

Die SSL Konfiguration erfolgt über die folgenden Einträge:

SSL=*true*

SSLRejectExpiredCert=false

Sie können während der Installation die grafische Konfiguration überspringen und gleichzeitig eine kommentierte „rccmd.cfg“ erzeugen, wenn Sie die Frage:

```
This is NOT an ITANIUM (IA-64) system [Y/n]?:
```

mit „n“ beantworten.

5.6.1 RCCMD mit eigenen SSL Zertifikaten

In diesem Abschnitt beschreiben wir, wie man ein eigenes SSL Zertifikat mit RCCMD nutzen kann, z. B. OpenSSL (http://www.openssl.org):

Sein Sie Ihre eigene Zertifizierungsstelle (CA)

Mit der Nutzung von OpenSSL ist es sehr einfach, sein eigener Zertifizierer zu werden. Nutzen Sie einfach diesen Befehl:

```
CA.pl –newca
```

Fertig! Vergewissern Sie sich, dass Sie einen gebräuchlichen CN (gewöhnlichen Namen) verwendet haben.

Erstellen des RCCMD Zertifikats

Nun müssen Sie Ihr Zertifikat für RCCMD erstellen. Da es für die Verifizierung den CN nutzt, sollte das Zertifikat diesen Namen auch enthalten, den Sie für das CA gewählt haben. Die private Schlüssel muss nicht verschlüsselt werden, um den RCCMD Client (Dienst) zu starten. Dafür nutzen wir die “-nodes” Option und den “-newreq” Befehl:

```
CA.pl –newreq –nodes
```

Signieren mit CA:

```
CA.pl –sign
```

Erstellen Sie nun eine leere Datei mit dem Namen “rccmd.pem”, und kopieren Sie die Zertifizierungsinformationen von “newcert.pem” (RCCMD Zertifikat), “newkey.pem” (Privater Schlüssel) und “cacert.pem” (CA) in diese Datei. Bitte beachten Sie, dass das exakte Kopieren erforderlich ist, damit Sie es ohne Probleme nutzen können.

Nutzung des eigenen RCCMD Zertifikats

Führen Sie die folgenden Schritte auf jedem RCCMD Client und Sender aus, um die Konfiguration abzuschliessen.

- Stellen Sie ein Backup von der existierenden “rccmd.pem” her
- Ersetzen Sie die “rccmd.pem” mit Ihrer eigenen
- Starten Sie den RCCMD Client neu
- Starten Sie den RCCMD Sender neu

6. RCCMD auf DEC VMS

Die UPS-Management Software CD beinhaltet die RCCMD Software. Die RCCMDVMS Installation kann wie die UNIX Installation durchgeführt werden, die im Kapitel 3.2.6 in diesem Handbuch beschrieben ist.

Achtung: **Der VMS Lizenz Schlüssel ist nicht auf der Standard CD enthalten und muss separat bestellt werden.**

Sie sollten sich vor der Installation vergewissern, dass der Port 6003 nicht in Gebrauch ist. Sie können dies mit dem Befehl « netstat –an » überprüfen. Wenn Sie einen anderen Port verwenden möchten, können Sie dies mit der Option « -p » für das Senden und Empfangen starten. Beachten sie, dass Sie dann diesen Port für jeden anderen Befehl im Netzwerk verwenden müssen. Folgen Sie den Anweisungen des nächsten Kapitels sorgfältig. Nutzen Sie das Handbuch für weitere Hilfe oder kontaktieren Sie Ihren UPS Software Händler.

Wichtig: **Die Alpha Version ist zur Open VMS 7.1 verlinkt. Nutzen Sie für Open VMS 6.x die Version 6.x in dem CD-Verzeichnis VMS.ALPHA.**

Installation:

- Verbinden Sie die Workstation mit dem Netzwerk.
- Melden Sie sich am VMS System mit dem SYSTEM Login an.

- Mounten Sie das CD-ROM-Verzeichnis, wenn DKA200 der Gerätename des CD-ROM Laufwerks ist:

$ MOUNT/OVERRIDE=IDENT DKA200: UPS UPS:

Dies ist ein System spezifischer Befehl. Nutzen Sie die VMS Hilfeseiten von Ihrem System oder Fragen Sie den System Operator, wenn Sie nicht wissen, wie man mounted.

- Starten Sie die VMS Installations-Prozedur mit: @SYS$UPDATE:VMSINSTAL
- oder: @SYS$UPDATE:VMSINSTAL <device>
- z.B.: @SYS$UPDATE:VMSINSTAL RCCMD DKA200: [VMS.ALPHA]

VMSINSTAL ist ein interaktives Script. Folgen Sie einfach den Installations-Anweisungen auf dem Bildschirm (alle Anweisungen sind zusätzlich in den Subjects 5-11 aufgelistet).

- Beantworten Sie mit YES: "* *Are you satisfied with the backup of your system disk [YES*]"
- Beantworten Sie: "* *Where will the distribution volumes be mounted*:" with your correct input device name, z.B.:

CDROM: *dka500: [VMS]* (your CDROM device and path [VMS], the device may be different on your system).

- Beantworten Sie*:"* Enter installation options you wish to use [none]:"* by pressing RETURN
- Bei*:"Please mount the first volume of the set on MKA300:." "* Are you ready?*"* Bitte legen Sie Ihre Disk oder CD-ROM in das Laufwerk und antworten mit YES.
- Tragen Sie den Lizenz Schlüssel Ihrer RCCMD Version ein
- Tragen Sie den kompletten Pfad des Zielverzeichnisses ein, z.B: *dka100: [ups]*
- Beantworten Sie: *"Would you like to start the RCCMD module automatically on your system".*
- Verlassen Sie die VMSINSTAL Prozedur mit RETURN bei "*Product:" prompt und bewegen Sie sich in das Zielverzeichnis (z.B.: dka100: [ups]).
- Nun installieren Sie die RCCMD Software im Sender Modus auf Ihrem RCCMD Server. Der RCCMD Server ist der Rechner, der mit der USV über den RS232-Port verbunden ist

DEC ALPHA CD Probleme: Wenn die CD nicht gemounted werden kann, oder Sie Probleme beim Starten des VMSINSTAL Scripts auf der DEC ALPHA Hardware haben, folgen Sie bitte diesen Anweisungen:

- Kopieren Sie das Archiv VMSA.ZIP (ALPHA directory) in ein temporäres Verzeichnis auf Ihrem System. COPY RCCMD.ZIP DKA100:[TEMP]

Wenn Sie kein ZIP-Programm auf Ihrer Workstation installiert haben sollten, müssen Sie einen System Wert anweisen: UNZIP==$DKA200:[VMS.ALPHA]UNZIP.EXE, wobei DKA200 Ihr CD-ROM Verzeichnis ist.

- Entpacken Sie Ihr VMS UPS Archiv:

SET DEF DKA100:[TEMP] UNZIP RCCMD.ZIP

- Starten Sie die VMS Installations Routine: @SYS$UPDATE:VMSINSTAL RCCMD DKA100:[TEMP]

Konfigurations-Prozedur:

Nach der Installation befinden sich 3 Befehls-Files auf Ihrem System:

- RCCMDSTART.COM: Der RCCMD Startbefehl sollte sich im VMS Startbefehl File befinden.
- RCCMD.COM: Befehls-File zum Starten von dem Programm, das Sie für Ihre Anforderungen entsprechend konfigurieren können.
- RCCMD_SHUTDOWN.COM: RCCMD-Befehls-File zum Herunterfahren von VMS.

Konfigurieren Sie RCCMD.COM wie folgt: “rccmd –l”, optional “rccmd –l-a (IP-Adresse des Senders)”, “-p (port, Standard ist 6003)”. Danach können Sie RCCMD mit “@rccmdstart” starten.

Prüfen Sie mit „show system“, ob ein RCCMD-Prozess vorhanden ist.

Der automatische Start von RCCMD sollte vom VMS Start-File initiiert werden. Fügen Sie folgende Zeile zu Ihrem Start-File hinzu:

$ @your_disk:[your_path]rccmdstart.com (e. g.: $ @dka100:[ups]rccmdstart.com)

Nach dem Reboot wird die UPS Software automatisch gestartet.

7. RCCMD auf MAC OS 9

Die Installation von RCCMD auf MAC OS 9 wird nicht länger unterstützt. Aktuell unterstützen wir RCCMD auf MAC OS 10.4 und höher.

Wir beschreiben die alte RCCMD Installation auf MAC OS 9. Die Installation kopiert automatisch einen Alias auf dem Desktop (rccmd configuration.url).

1.

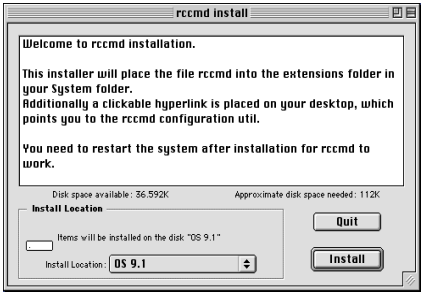

rccmd install
Welcome to rccmd installation.
This installer will place the file rccmd into the extensions folder in your System folder.
Additionally a clickable hyperlink is placed on your desktop, which points you to the rccmd configuration util.
You need to restart the system after installation for rccmd to work.
Disk space available: 36.592K
Approximate disk space needed: 112K
Install Location
Items will be installed on the disk "OS 9.1"
Install Location: OS 9.1
Quit
Install

Abb. 88: Mac OS RCCMD Installations-Start

Nach der Installation der RCCMD Archive, erhalten Sie folgende Meldung:

Nach dem Reboot des Computers kann die Konfiguration beginnen. Um dies auszuführen, klicken Sie auf “rccmd configuration.url”. Ein Standard Webbrowser wird gestartet.

2.

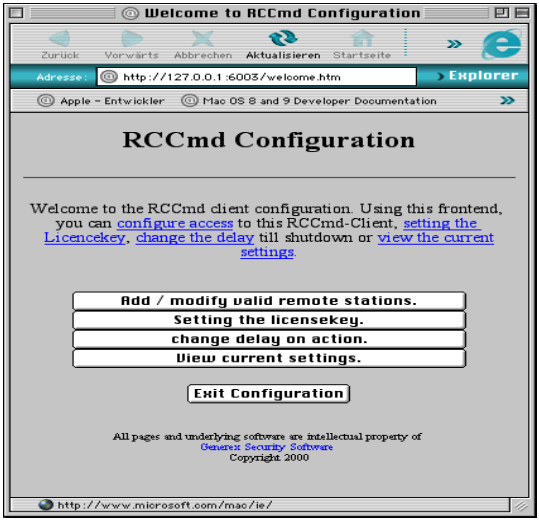
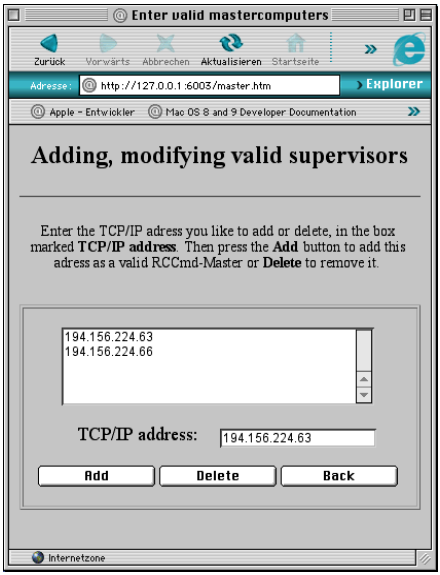


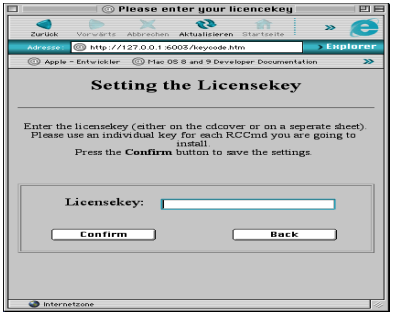
Abb. 89: Mac OS RCCMD Konfiguration

Wir empfehlen die Menü-Optionen von oben nach unten auszuführen.



Diese Option ermöglicht das Eintragen von IP-Adressen der RCCMD Sender, die das Shutdown Signal zu den Remote Computer senden (RCCMD Clients). Die Konfiguration des RCCMD Senders ist abhängig von der UPSMAN Konfiguration. Bitte schauen Sie in das RCCMD Windows Kapitel in diesem Handbuch. Tragen Sie die entsprechenden IP-Adressen in das Feld “TCP/IP address” ein und klicken auf “Add”.

Abb. 90: Mac OS hinzufügen/modifizieren gültiger Remote Stations



Bitte tragen Sie den Lizenz-Schlüssel ein, und bestätigen Sie mit “Confirm”. Mit “Back” gelangen Sie zurück zum Hauptmenü.

Abb. 91: Mac OS Lizenz Schlüssel Eintrag

Bitte beachten Sie die Lizenzbedingungen für RCCMD Sender und Lauscher (Clients). Die Standard Version der MAC OS UPS Management Software, kann unbegrenzt RCCMD Signale zu RCCMD Clients senden. Pro Lizenz können Sie **einen** RCCMD Client herunterfahren. Bitte kontaktieren Sie Ihren USV-Händler, wenn Sie weitere Lizenzen benötigen.

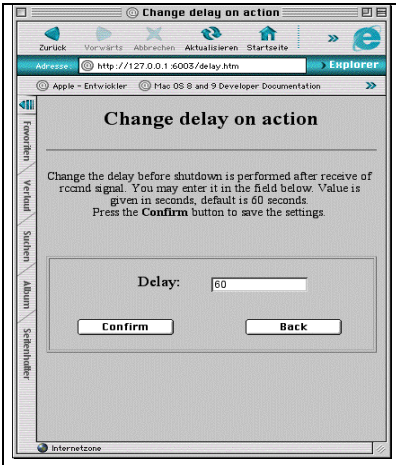


Abb. 92: Mac OS Verzögerungs-Option

Das Menü “Change delay on action” ermöglicht dem Benutzer das Eintragen einer Verzögerung in Sekunden, bevor der Shutdown eines RCCMD Clients initiiert wird, nach dem ein entsprechendes Signal empfangen wurde. Der Standard ist 60 Sekunden, mit “Confirm” bestätigen Sie Ihre Veränderung.

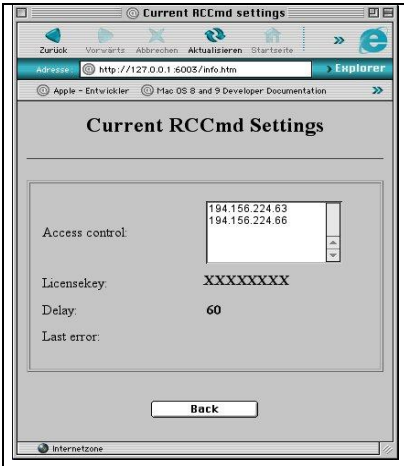


Abb. 93: Mac OS Aktuelle Einstellungen

Hier sehen Sie die aktuellen Einstellungen. In dem Feld “Access control” sehen Sie die IP-Adressen der RCCMD Sender, die authorisiert sind, RCCMD Signale zu senden. Im Feld “Last error” werden die letzten RCCMD Fehler gemeldet. Mit “Back” gelangen Sie zurück zum Hauptmenü. Nach einer erfolgreichen Installation, startet RCCMD generell automatisch. Wenn dies nicht erwünscht ist, entfernen Sie die korrespondierende System Erweiterung aus dem System Erweiterungs Ordner.

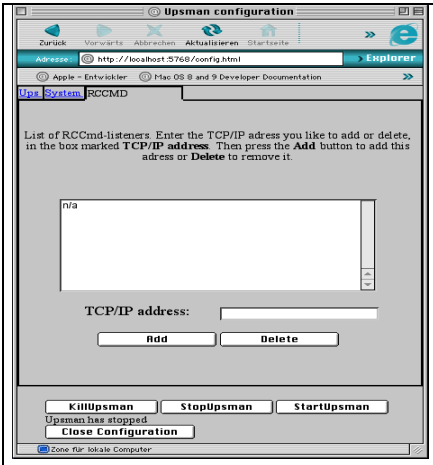


Abb. 94: Mac OS hinzufügen von RCCMD Empfängern (RCCMD Clients)

Bitte starten Sie den Alias “upsman configuration.url”, wie im vorherigen Kapitel beschrieben. Danach öffnet sich das Fenster “RCCMD Clients”.

Bitte tragen Sie die IP-Adressen der RCCMD Clients (Lauscher) in das Feld “TCP/IP address” und klicken Sie auf “Add”.

Genau wie bei der UPSMAN Windows Konfiguration empfehlen wir, die Anzahl der RCCMD Empfänger zu limitieren, da ohne Eintrag in der Empfänger Liste, alle RCCMD Empfänger (Clients) im Netzwerk einen Shutdown durchführen würden (abhängig vom Lizenz Status). Die RCCMD Konfiguration ist nun abgeschlossen.

8. RCCMD auf MAC OS 10.X

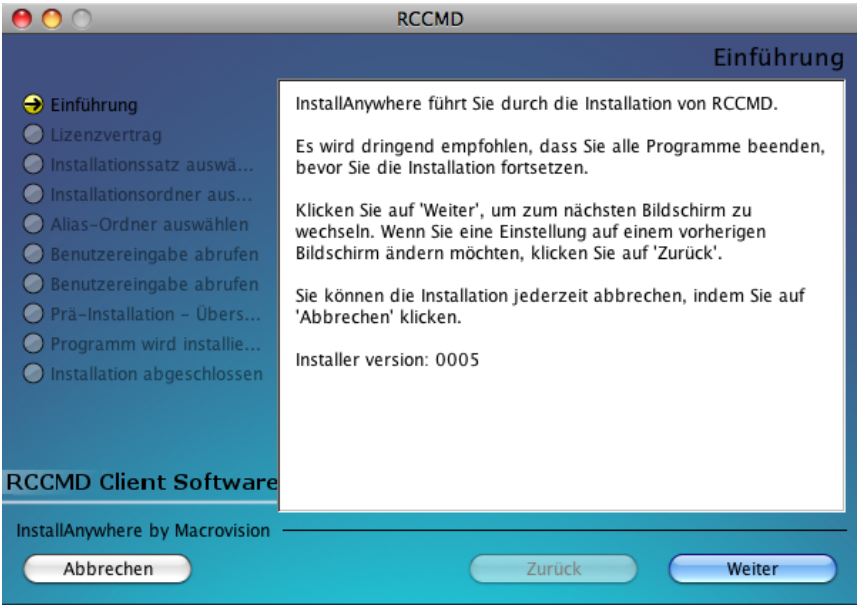

RCCMD
Einführung
Einführung
Lizenzvertrag
Installationssatz auswä...
Installationsordner aus...
Alias-Ordner auswählen
Benutzereingabe abrufen
Benutzereingabe abrufen
Prä-Installation - Übers...
Programm wird installie...
Installation abgeschlossen
InstallAnywhere führt Sie durch die Installation von RCCMD.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die Installation fortsetzen.
Klicken Sie auf 'Weiter', um zum nächsten Bildschirm zu wechseln. Wenn Sie eine Einstellung auf einem vorherigen Bildschirm ändern möchten, klicken Sie auf 'Zurück'.
Sie können die Installation jederzeit abbrechen, indem Sie auf 'Abbrechen' klicken.
Installer version: 0005
RCCMD Client Software
InstallAnywhere by Macrovision
Abbrechen
Zurück
Weiter

Abb. 95: RCCMD Installations-Willkommen

Sie benötigen einen speziellen Lizenz-Schlüssel für die RCCMD Software, den Sie an dem “RX3” im ersten Teil des Schlüssels erkennen können. In den meisten Fällen muss die Lizenz separat bestellt werden.

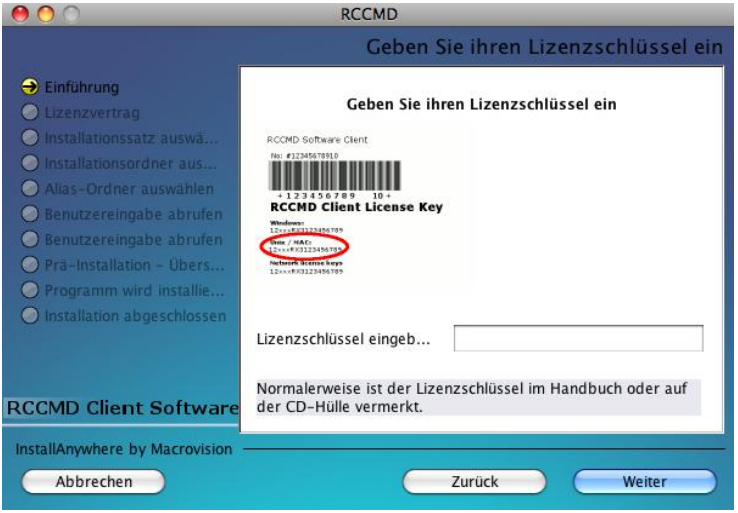


Abb. 96: RCCMD Lizenz Schlüssel Eingabe

Abb. 97: Prä-Installations-Übersicht

Fügen Sie die IP-Adresse des RCCMD Servers hinzu, der authorisiert ist, ein Shutdown Signal zu diesem Client zu senden.

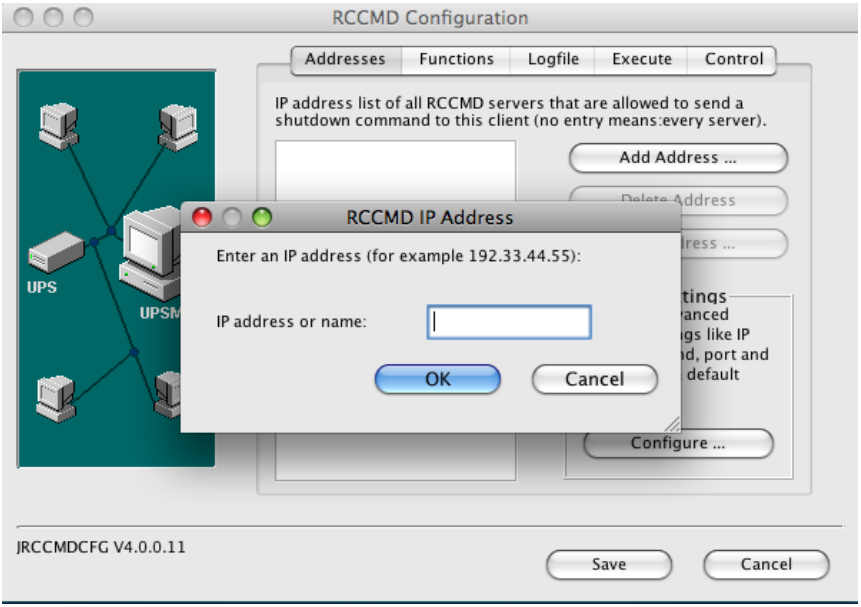


Abb. 98: RCCMD IP Adressen Fenster

Achtung:

Wenn Sie keine Adresse eintragen, ist automatisch jeder Server authorisiert, ein Shutdown Signal zu senden. Wenn mehr als ein CS121 oder UPSMAN im Netzwerk existieren, also eine Redundanz Situation, müssen Sie mehrere Adressen als authorisierte Sender eintragen.

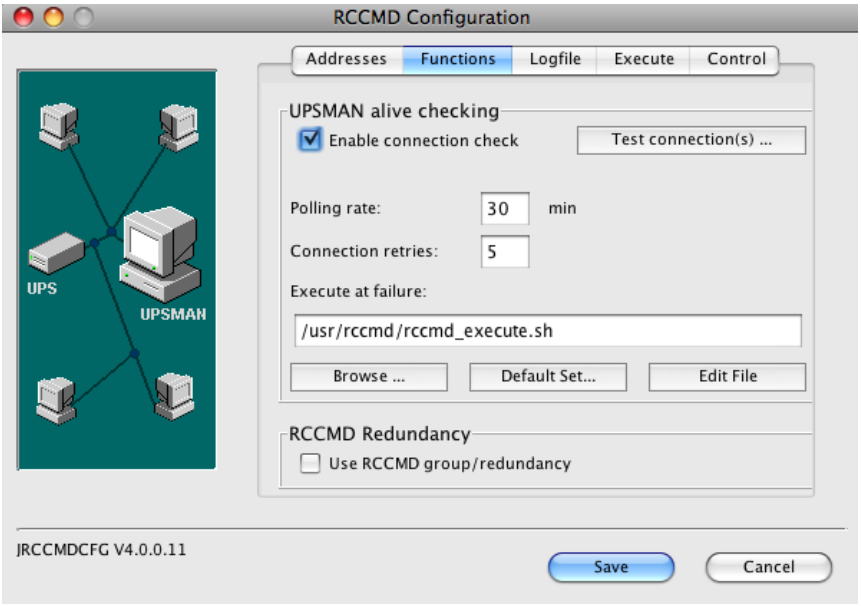


Abb. 99: RCCMD Konfigurations-Fenster „Functions“

Wenn Sie die Funktion “UPSMAN Alive Checking” nutzen möchten (empfohlen), haken Sie die entsprechende Box an. Dieser Check ist ein Signal, dass an den CS121 oder UPSMAN via Port 5679 gesendet wird, um zu prüfen, ob der UPSMAN noch USV Daten hat. Wenn nicht, wird das Script File “rccmd_notalive.sh” ausgeführt, das eine entsprechende Nachricht als Pop-Up bringt. Die *Polling Rate* (Standard 30 Minuten) definiert den Interval der UPSMAN Abfrage, *connect retries* (Verbindungswiederholungen, Standard 5) bedeutet, das nach 5 erfolglosen Verbindungsversuchen ein Alarm ausgelöst wird.

Die Funktion “Use RCCMD Traps” ermöglicht UPSMAN/RCCMD/UNMS Meldungen, die den USV Status als Nachricht anzeigt. Wenn aktiviert, wird diese Funktion eine lokale Nachricht bringen, wenn der USV Status des UPSMAN/RCCMD Servers sich verändert.

Wenn Sie auf “Test connections…” klicken, wird das UPSMAN Alive Checking von der eingetragenen IP-Adresse gestartet (der Port 5679 wird getestet).

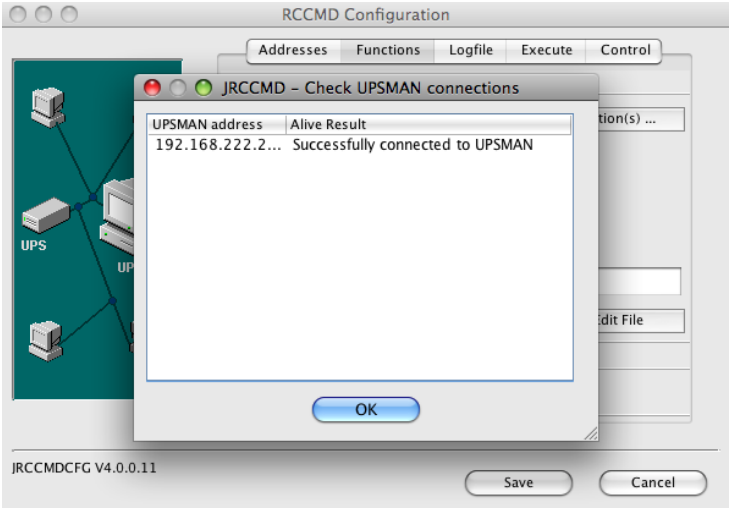


Abb. 100: RCCMD Check UPSMAN Verbindungen

Wenn Sie auf “Browse…” klicken, werden Sie eine Auswahl der Standard SH-Files erhalten.

Wenn Sie auf „Default Setting“ klicken, werden Sie zurück zum „rccmd_notalive.sh“ File gelangen.

Bei einem Fehler von dem UPSMAN Alive Check können Sie eine auszuführende Datei konfigurieren oder das Standard File editieren.

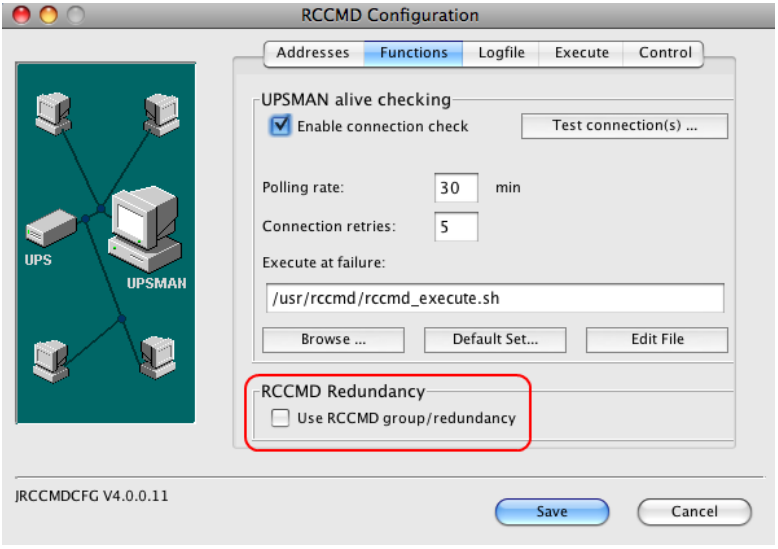


Abb. 101: RCCMD Redundanz

Bei der USV Installation bietet RCCMD eine Redundanz Management Funktion wie folgt an:

Jede USV muss mit einem CS121 oder einem UPSMAN Software Computer ausgestattet sein. Wenn Sie die Box “Use RCCMD group/redundancy” anhaken, gelangen Sie zu einem Menü, welcher CS121/UPSMAN diesen RCCMD Client versorgt. Z.B.: Wenn 4 CS121/UPSMAN in 4 USVen installiert sind, dann kann jeder ein Shutdown Signal zu diesem RCCMD Client absetzen.

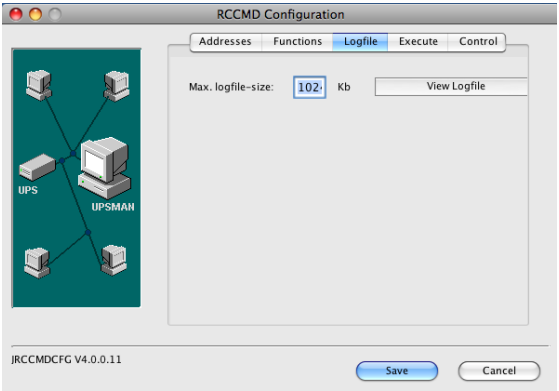


Abb. 102: RCCMD Konfigurations-Fenster „Logfile“

Sie können die Log File Grösse konfigurieren und die auszuführenden Files editieren.

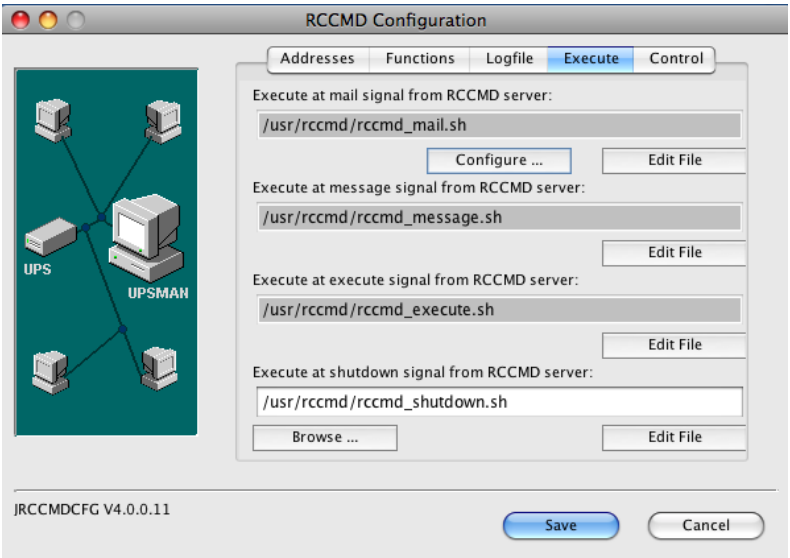


Abb. 103: RCCMD Konfigurations-Fenster „Execute“

Wenn Sie auf “Configure…” klicken, können Sie die Email Einstellungen vornehmen und die Mailfunktion von RCCMD nutzen.

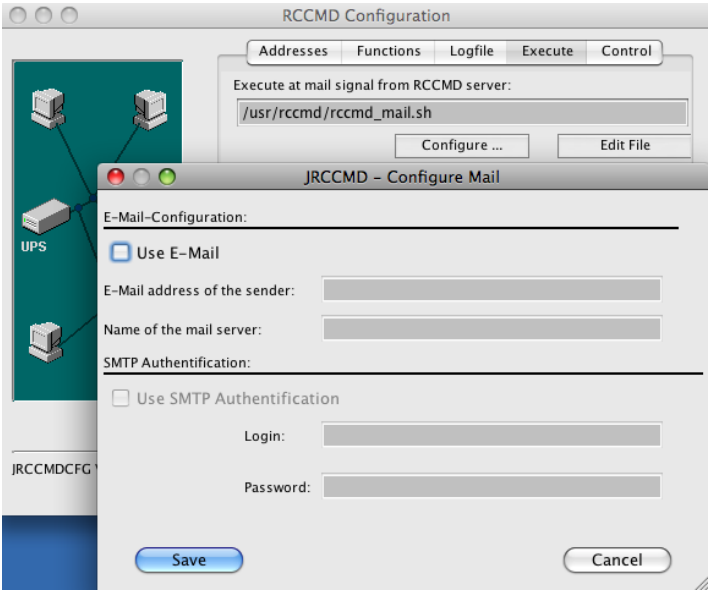


Abb. 104: RCCMD E-Mail-Konfiguration

Ab der RCCMD Version 4.0.2.0 gibt es auch eine grafische Konfiguration der Shutdown Sequenz.

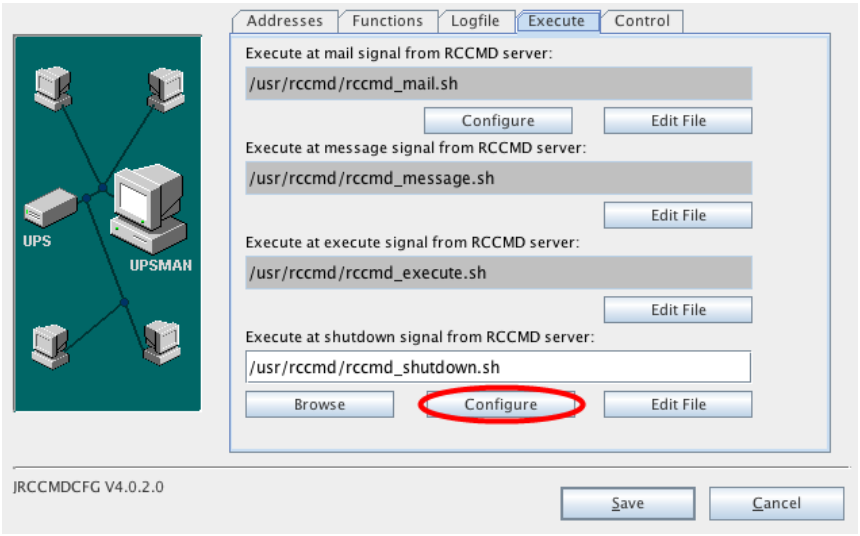


Abb. 105: Konfiguration – RCCMD Shutdown.sh

Klicken Sie auf „Configure“, um die Shutdown Sequenz zu öffnen.

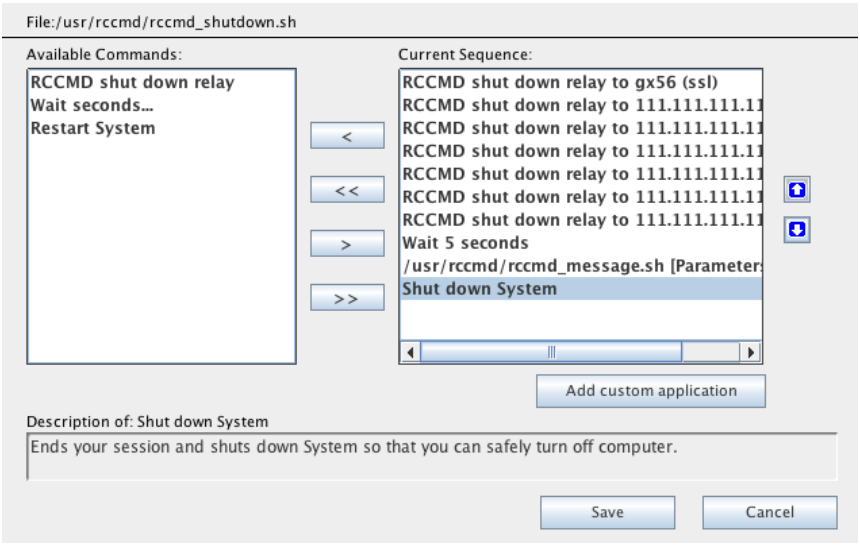


Abb. 106: Konfiguration – RCCMD Shutdown Sequenz

Die folgenden Befehle sind für die Shutdown Sequenz Konfiguration erhältlich:

RCCMD shutdown relay: Leitet einen RCCMD Shutdown Befehl an eine andere Workstation weiter (siehe auch Kapitel 5.4, Seite 75).

Wait seconds...: Warten eines Zeitraums in Sekunden, bis das nächste Kommando ausgeführt wird.

Restart System: Beendet Ihre Sitzung, fährt das System herunter und startet es neu.

Shutdown System: Beendet Ihre Sitzung und fährt das System herunter, sodass Sie sicher die Stromzufuhr unterbrechen können.

Über den „Control“ Button gelangen Sie zu der folgenden Maske:

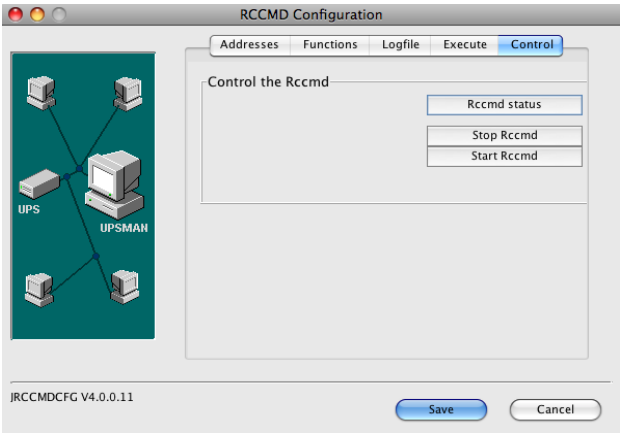


Abb. 107: RCCMD Control

9. RCCMD auf Citrix XEN Server

Die RCCMD Software auf XEN Server ist ein auf Linux basierter TCP Client, der das Empfangen von Shutdown Signalen von der UPSMAN Software, CS121 SNMP Adapter oder jeder anderen lizensierten RCCMD Anwendung.

RCCMD auf XEN Server läuft auf GNU Linux 2.6.18 oder höher, das die Basis der 2008 XEN Serverplattform ist.

Für die Installationsanleitung von RCCMD, schauen Sie bitte in das Kapitel 5.3 auf Seite 64. Im Folgenden beschreiben wir nur die speziellen Aspekte, die nur für XEN Server relevant sind.

Installation:

Da der XEN Server keine grafische Oberfläche unterstützt, der Download der RCCMD Software für XEN Server von der GENEREX Webseite oder anderen Seiten, ist es nicht einfach, es sei denn, Sie haben einige Extra Tools installiert, z. B. den Befehlszeilen-Browser *Wget*.

Eine zusätzliche Schwierigkeit ist, dass auf XEN Server kein FTP Server aktiv ist, sodass ein Transfer eines RCCMD Download-Paketes auch nicht möglich ist. Darum empfehlen wir, eine lokale Schnittstelle, z.B. ein CD-ROM Laufwerk, auf Ihrem XEN Server zu nutzen oder mit einem USB Stick zu arbeiten.

- Laden Sie RCCMD mit ihrer Lizenznummer (nicht älter als 2 Jahre) von der GENEREX Webseite herunter, und extrahieren Sie das TAR File. Kopieren Sie die Files auf eine CD-R, und legen Sie die CD in das Laufwerk auf Ihrem XEN Server. Alternativ können Sie die UPSMAN CD-ROM Version 5.48 oder höher nutzen.

- Loggen Sie sich als Root ein, und mounten Sie die CD-ROM auf Ihrem XEN Server: Geben Sie `mount/dev/cdrom/media` ein. Sie werden folgende Antwort vom System erhalten: `mount: block device /dev/cdrom is write protected, mounting read-only`
- Wechseln Sie zu dem CD-ROM Verzeichnis mit: `cd/media` – mit `ls` können Sie sich die Files der CD-ROM anzeigen lassen. Wechseln Sie in das Verzeichnis UNIX (UPSMAN CD-ROM) oder GENEREX. Darin befindet sich das Installations-File "install".
- Starten Sie die Installation mit der Eingabe: `./install` und folgen Sie den Anweisungen auf dem Bildschirm, die identisch zur Installation von RCCMD auf UNIX ist.
- Nach dem die Installation beendet ist, wird ein neuer Prozess auf Ihrem XEN Server laufen: `:/rccmd -l` , was bedeutet, dass das System nun bereit ist.
- **Achtung**: Der XEN Server hat standardmässig eine aktive Firewall, die keine "remote" RCCMD Signale zulässt. Um die Firewall zu öffnen, müssen die *iptables* (`/etc/sysconfig#`) editiert werden.

Firewall Konfiguration:

Fügen Sie die folgenden *Lines* in `/etc/sysconfig/iptables` **vor** der letzten *REJECT* Regel hinzu:

```
-A RH-Firewall-1-INPUT -p udp --dport 6003 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp --dport 6003 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/sysconfig/iptables" [readonly] 25L, 1215C
```

Abb. 108: Firewall Konfiguration

Starten Sie die *iptables* wie folgt neu:

```
/etc/init.d/iptables restart
```

RCCMD ist nun im Lauscher-Modus konfiguriert, und wird das File *shutdown.sh* auf Ihrem XEN Server starten, wenn ein CS121 Adapter oder UPSMAN ein RCCMD Shutdown

Signal sendet. Das File *shutdown.sh* führt ein *init0 shutdown* auf Ihrem XEN Server aus. Ändern Sie das File, wenn Sie eine andere Shutdown Prozedur verwenden möchten.

Hinweis:

Es wird empfohlen, RCCMD auch auf den virtuellen Gast-systemen zu installieren und diese VOR dem physikalischen Hostrechner herunterzufahren. Dies garantiert ein sauberes Herunterfahren der virtuellen Maschinen und verhindert den möglichen Datenverlust durch ein nicht erfolgreiches Hibernating.

10. RCCMD auf VMware

VMware ist Hersteller für Virtualisierungslösungen und vertreibt verschiedene Ausprägungen solcher Produkte. RCCMD kann neben den virtuellen Systemen auch die VMware physikalischen Systeme herunterfahren. Eine Beschreibung, was auf den jeweiligen Produkten zu beachten ist, finden Sie im folgenden Kapitel.

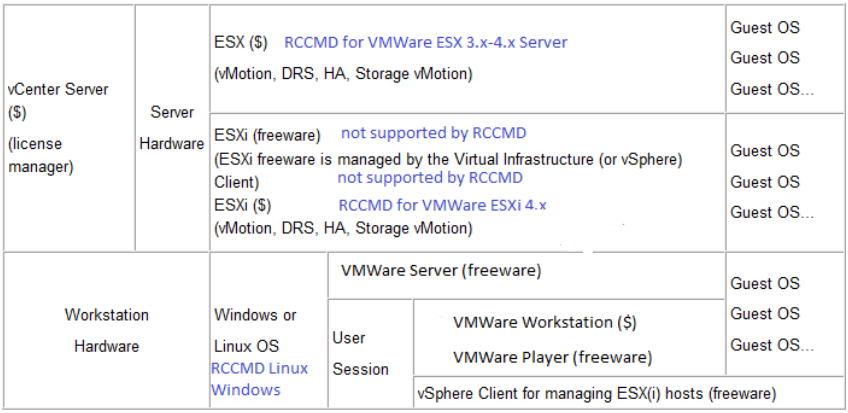


Abb. 109: VMware Products

RCCMD ist in der Lage, die ESX ($) und ESXi Produkte herunterzufahren.

Die RCCMD Software auf VMware wird unterschieden für „VMware ESX“ und „VMware ESXi“. Der VMware ESX ist immer kostenpflichtig und enthält einen integrierten Linux Desktop. VMware ESXi ist auch kostenlos erhältlich. VMware ESXi ist ein in ein anderes Betriebssystem eingebettetes System, mit einer per Webbrowser zu bedienenden Oberfläche. Bitte lesen Sie zu den jeweiligen Unterschieden in der Bedienung mit RCCMD die in den jeweiligen Kapiteln enthaltenen Installations- und Bedienungshinweise.

10.1 RCCMD auf VMware ESX

Die RCCMD Software auf VMware ESX ist ein auf Linux basierter TCP Client, der das Empfangen von Shutdown Signalen von der UPSMAN Software, CS121 SNMP Adapter oder jeder anderen lizensierten RCCMD Anwendung ermöglicht.

RCCMD auf VMware ESX läuft auf GNU Linux 2.6.18 oder höher, das die Basis der VMware ESX Plattform ist.

Für die Installationsanleitung von RCCMD schauen Sie bitte in das Kapitel 5. RCCMD auf UNIX. Im Folgenden beschreiben wir nur die speziellen Aspekte, die nur VMware ESX relevant sind.

Installation:

Da der VMware ESX keine grafische Oberfläche besitzt, empfehlen wir, eine lokale Schnittstelle, z. B. ein CD-ROM Laufwerk, auf Ihrem VMware ESX zu nutzen oder mit einem USB Stick zu arbeiten um RCCMD zu installieren.

- Laden Sie RCCMD mit ihrer Lizenznummer (nicht älter als 2 Jahre) von der GENEREX Webseite herunter, und extrahieren Sie das TAR File. Kopieren Sie die Files auf eine CD-R, und legen Sie die CD in das Laufwerk auf Ihrem ESX Server. Alternativ können Sie die UPSMAN CD-ROM Version 5.48 oder höher nutzen.
- Loggen Sie sich als Root ein, und mounten Sie die CD-ROM auf Ihrem VMware ESX Computer: Geben Sie `mount/dev/cdrom` ein.
- Wechseln Sie zu dem CD-ROM Verzeichnis mit: `cd/mnt/cdrom` – mit `ls` können Sie sich die Files der CD-ROM anzeigen lassen. Wechseln Sie in das Verzeichnis UNIX (UPSMAN CD-ROM) oder GENEREX. Darin befindet sich das Installations-File “install”.
- Starten Sie die Installation mit der Eingabe: `./install` und folgen Sie den Anweisungen auf dem Bildschirm, die identisch zur Installation von RCCMD auf UNIX ist.
- Nach dem die Installation beendet ist, wird ein neuer Prozess auf Ihrem VMware ESX laufen: `:/rccmd -l` , was bedeutet, dass das System nun bereit ist.
- **Achtung:** Der VMware ESX hat standardmässig eine aktive Firewall, die keine RCCMD Signale zulässt.

Firewall Konfiguration:

Die folgende Firewall Konfiguration auf dem VMware ESX ist erforderlich, um RCCMD Signale empfangen zu können:

```
esxcfg-firewall -o 6003,tcp,in,RCCMD
```

Starten Sie den Firewall Service neu, um Ihre Einstellungen zu speichern:

```
service firewall restart
```

RCCMD ist nun im Client-Modus konfiguriert und wird das File *shutdown.sh* auf Ihrem VMware ESX starten, wenn ein CS121 Adapter oder UPSMAN ein RCCMD Shutdown Signal sendet. Das File *shutdown.sh* führt ein *init 0 shutdown* auf Ihrem VMware ESX aus. Ändern Sie das File, wenn Sie eine andere Shutdown Prozedur verwenden möchten.

Hinweis:

Es wird empfohlen, RCCMD auch auf den virtuellen Gast-systemen zu installieren und diese VOR dem physikalischen Hostrechner herunterzufahren. Dies garantiert ein sauberes Herunterfahren der virtuellen Maschinen und verhindert den möglichen Datenverlust durch ein nicht erfolgreiches Hibernating.

10.2 RCCMD auf VMWARE ESXi

Die RCCMD Software auf VMware ESXi ist ein auf Linux basierter TCP Client (TCP/IP Empfänger), der das Empfangen von Shutdown Signalen von der UPSMAN Software, CS121 SNMP Adapter oder jeder anderen lizensierten RCCMD Anwendung ermöglicht.

Achtung:

RCCMD wird nur dann unterstützt, wenn der VMWARE ESXi Host *NICHT* mit einem *kostenlosen* ESXi-Lizenzschlüssel installiert wurde!

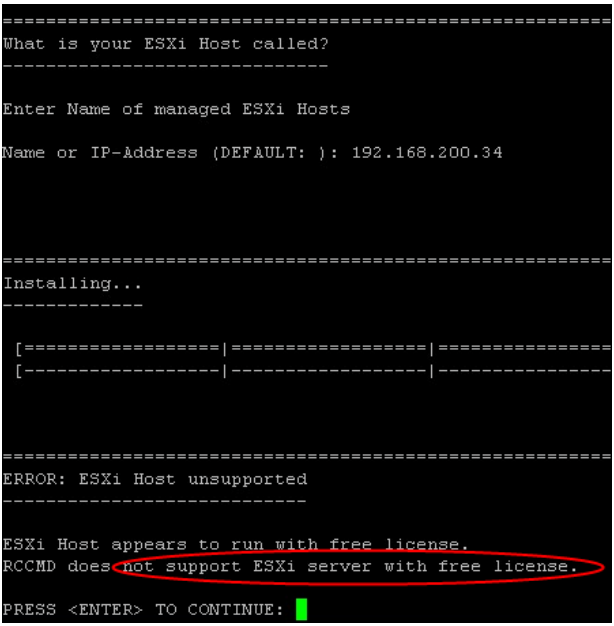

What is your ESXi Host called?
Enter Name of managed ESXi Hosts
Name or IP-Address (DEFAULT:): 192.168.200.34
Installing...
ERROR: ESXi Host unsupported
ESXi Host appears to run with free license.
RCCMD does not support ESXi server with free license.
PRESS <ENTER> TO CONTINUE:

Abb. 110: ESXi Lizenz-Fehlermeldung bei kostenloser ESXi Lizenz

Die VMware ESXi bietet den vSphere Management Assistant (vMA) 4.0 oder 4.1 als Schnittstelle für externe Anwendung an, in welcher der RCCMD Client läuft. D.h. der RCCMD Client in der vMA erhält Signale zum Shutdown vom CS121 und sendet das Shutdown Kommando an den ESXi Server über die vMA Schnittstelle weiter.

Der vMA Assistent bietet ein Management-Interface an, mit dem der VMware ESXi automatisch per Skript gesteuert werden kann.

Auf dem vMA wird RCCMD installiert, dabei erkent der RCCMD-Installer automatisch, dass die Installation auf einer VMware Anwendung ausgeführt wird und installiert entsprechend angepasste Scriptdateien für den Shutdown.

Achtung: **RCCMD wird nur für die original VMware unterstützt, nicht für „gehärtete“ oder OEM Versionen von VMware.**

Folgende Voraussetzungen sind für die Installation erforderlich:

- Auf dem ESXi Hypervisor läuft in einer virtuellen Maschine die vMA.
- Die vMA ist installiert und konfiguriert, Tipp: vma_41_guide.pdf S.13ff

  http://www.vmware.com/support/developer/vima/vma41/doc/vma_41_guide.pdf
- Ein vSphere-Client ist auf einer Workstation installiert

- Ein SCP/SFTP Client wird benötigt um die RCCMD-Installationsdateien auf den vMA kopieren zu können.

ESXi Host Konfiguration

RCCMD sendet den Shutdownbefehl von der vMA an den ESXi Host.

Tipp: Mit dem vSphere-Client kann jeder Host so konfiguriert werden, dass dieser vor dem Herunterfahren seine Gastsysteme sauber herunterfährt. Auf den Gastsystemen müssen hierfür die VMware-Tools installiert sein.

Hinweis:

Die Funktion des automatischen Herunterfahrens von Gastsystemen ist NUR gegeben, wenn die VMWare Tools installiert wurden. Dies garantiert allerdings nicht, dass die damit heruntergefahrenen Gast-Betriebssysteme auch ohne Datenverlust neustarten. Um dieses geringe Risiko auszuschliessen, empfehlen wir, auf jedem virtuellen Betriebsystem RCCMD zu installieren und VOR dem ESXi Host per RCCMD Shutdown herunterzufahren.

Shutdown-Konfiguration der virtuellen Maschinen auf dem ESXi

Wählen Sie im vSphere-Client Ihren Host (1) aus, klicken Sie auf “Konfiguration” (2), und markieren Sie “VM starten/herunterfahren” (3). Klicken Sie nun auf vMA (4) und oben rechts auf “Eigenschaften (5).

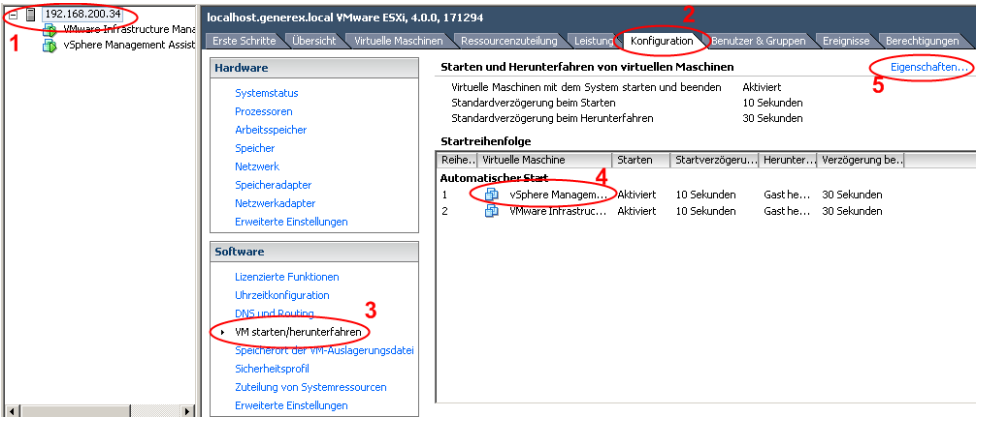


Abb. 111: vSphere-Client Konfiguration

Wählen Sie im Eigenschaften-Dialog den vMA aus, und setzen Sie seine Werte wie abgebildet auf 10 Sekunden Startverzögerung und 30 Sekunden Verzögerung beim Herunterfahren.

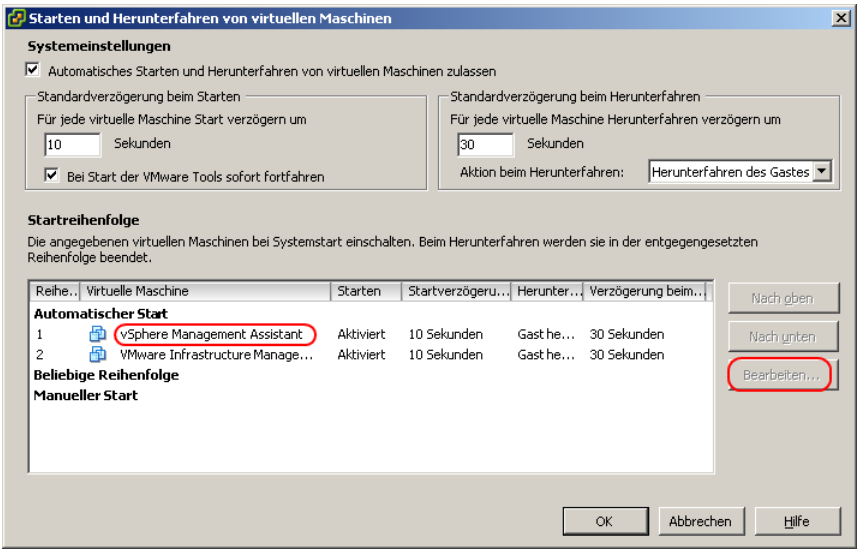


Abb. 112: vSphere-Client Autostart-Konfiguration

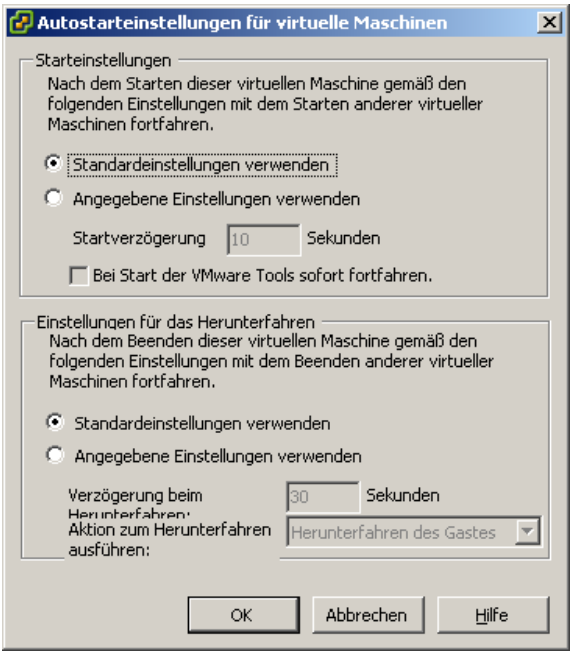


Abb. 113: vSphere-Client Autostart-Verzögerung

Die Verzögerungszeiten für die Gastsyysteme die auf dem ESXi laufen und mit dem Host heruntergefahren werden sollen, können abweichen und müssen individuell eingerichtet

werden. Die Dauer, die der Server dann für den Shutdown benötigt, wird dadurch enstprechend vergrössert.

RCCMD Installation:

RCCMD wird im Download als TAR Datei geliefert. Kopieren Sie die Datei RCCMDinst.tar mit Hilfe des SCP Clients (SFTP) auf den vMA.

- Loggen Sie sich auf der vMA ein, z.B. mit Putty.
- Erstellen Sie z. B. mit „mkdir“ ein temporäres Verzeichnis z.B. mit dem Namen „RCCMD“.
- Entpacken Sie die tar-Datei mit: `tar –xvf RCCMDinst.tar`

Es entstehen folgende Dateien nach dem Entpackvorgang:

```
[root@vMA41 ~]# cd /home/vi-admin/
[root@vMA41 ~]# mv RCCMD/ tmp
[root@vMA41 ~]# ls
rccmdinst.tar  tmp
[root@vMA41 ~]# mkdir RCCMD
[root@vMA41 ~]# mv rccmdinst.tar RCCMD/
[root@vMA41 ~]# cd RCCMD/
[root@vMA41 RCCMD]# tar -xvf rccmdinst.tar
gpg-pub.txt
installer.info
installer.properties
installRCCMD.bin
installRCCMD.bin.asc
installRCCMD.bin.md5
versionOEM12.xml
[root@vMA41 RCCMD]# ls
gpg-pub.txt     installer.properties  installRCCMD.bin.asc  rccmdinst.tar
installer.info  installRCCMD.bin      installRCCMD.bin.md5  versionOEM12.xml
[root@vMA41 RCCMD]#
```

Abb. 114: Installationsvorbereitung

Starten Sie die Installation mit dem Aufruf: `./installRCCMD.bin`

```
[root@vMA41 ~]# ls
RCCMD
[root@vMA41 ~]# cd RCCMD/
[root@vMA41 RCCMD]# ./installRCCMD.bin
```

Abb. 115: Ausführung der Binärdatei

Wählen Sie die Sprache aus, und drücken Sie die Eingabetaste.

[root@vMA41 RCCMD]# ./install_RCCMD.bin
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Launching installer...
Graphical installers are not supported by the VM. The console mode will be used instead...
Choose Locale...
1- Deutsch
->2- English
3- EspaÃ±ol
4- FranÃ§ais
5- Italiano
6- PortuguÃªs
CHOOSE LOCALE BY NUMBER: 1
RCCMD (created with InstallAnywhere)
Preparing CONSOLE Mode Installation...
EinfÃ¼hrung
InstallAnywhere fÃ¼hrt Sie durch die Installation von RCCMD-Client.
Es wird dringend empfohlen, dass Sie alle Programme beenden, bevor Sie die
Installation fortsetzen.
Beantworten Sie die Eingabeaufforderungen, um mit dem jeweils nÃ¤chsten Schritt
der Installation fortzufahren. Wenn Sie eine Einstellung in einem vorherigen
Schritt Ã¤ndern mÃ¶chten, klicken Sie auf 'ZurÃ¼ck'.
Sie kÃ¶nnen die Installation jederzeit abbrechen, indem Sie auf 'Beenden'
klicken.
DRÃCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 116: Sprachauswahl

Geben Sie den RCCMD Lizenzschlüssel, den Hostnamen bzw. die IP-Adresse des ESXi Host und das Root-Passwort ein.

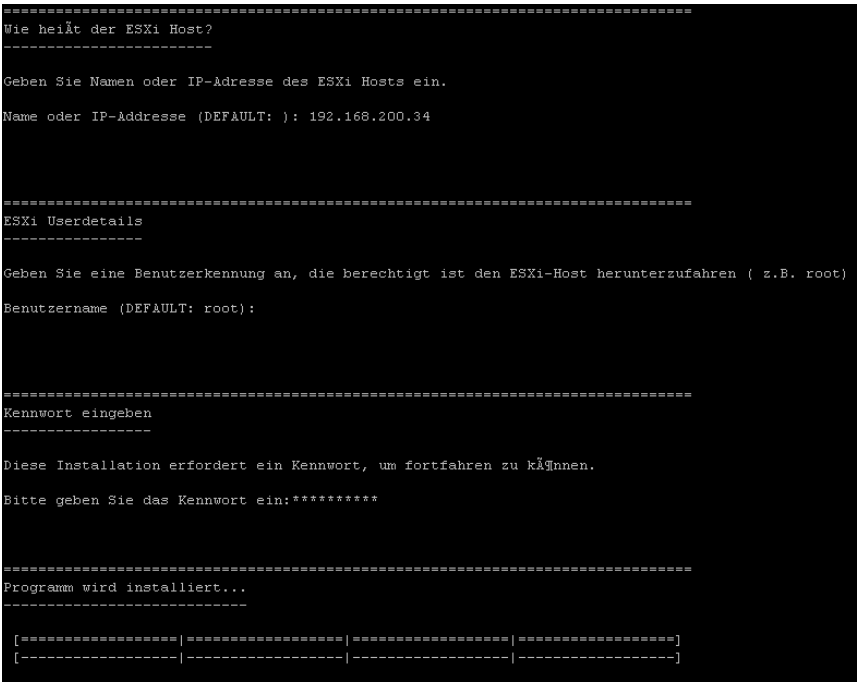

Wie heiÃt der ESXi Host?
Geben Sie Namen oder IP-Adresse des ESXi Hosts ein.
Name oder IP-Addresse (DEFAULT:): 192.168.200.34
ESXi Userdetails
Geben Sie eine Benutzerkennung an, die berechtigt ist den ESXi-Host herunterzufahren (z.B. root)
Benutzername (DEFAULT: root):
Kennwort eingeben
Diese Installation erfordert ein Kennwort, um fortfahren zu kÃ¶nnen.
Bitte geben Sie das Kennwort ein:**********
Programm wird installiert...

Abb. 117: Interaktive Eingaben – ESXi Userdetails, Kennwort

Automatische Firewall Konfiguration

RCCMD benötigt den Port 6003 (TCP und UDP) für eingehende IP-Pakete, bei Nutzung von „Check Alive“ Funktion auch TCP Port 5769 wird automatisch während der Installation freigeschaltet.

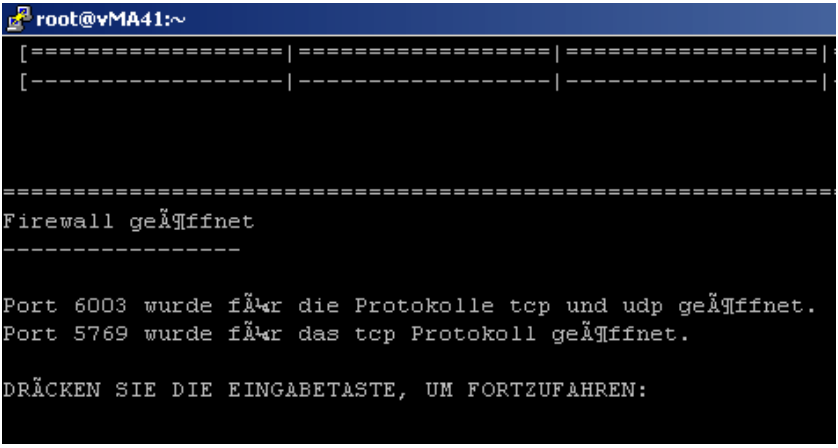

root@vMA41:~
Firewall geÃ¶ffnet
Port 6003 wurde fÃ¼r die Protokolle tcp und udp geÃ¶ffnet.
Port 5769 wurde fÃ¼r das tcp Protokoll geÃ¶ffnet.
DRÃCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:

Abb. 118: Installer meldet das Firewall Port 6003 und 5769 geöffnet wurden

Soll RCCMD automatisch bei Systemstart ausgefÃ¼hrt werden?
->1- OK
2- Abbrechen
GEBEN SIE DIE NUMMER DER GEWÄNSCHTEN KOMPONENTE AN, ODER DRÄCKEN SIE DIE EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ÄBERNEHMEN:
RCCMD-Konfiguration erforderlich
Eine Konfiguration des RCCMD ist erforderlich. Dazu muss die "/usr/rccmd/rccmd.cfg" bearbeitet werden.
Sollten Sie entscheiden den RCCMD mit der Standardkonfiguration zu starten, ist es von jeder Netzwerkadresse aus mÃ¶glich an diesen Nachrichten zu senden. Bitte richten Sie eine oder mehrere IP-Adressen ein, die berechtigt sein sollen diesem RCCMD Nachrichten zu senden.
DRÄCKEN SIE DIE EINGABETASTE, UM FORTZUFAHREN:
RCCMD jetzt starten?
Soll RCCMD jetzt gestartet werden?
Zum manuellen Starten verwenden Sie: "/usr/rccmd/rccmdctl start"
->1- OK
2- Abbrechen
GEBEN SIE DIE NUMMER DER GEWÄNSCHTEN KOMPONENTE AN, ODER DRÄCKEN SIE DIE EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ÄBERNEHMEN:
Installation abgeschlossen
Herzlichen GlÃ¼ckwunsch. RCCMD-Client wurde erfolgreich im folgenden Verzeichnis installiert:
/usr/rccmd
DRÄCKEN SIE DIE EINGABETASTE, UM DEN INSTALLER ZU BEENDEN:
[root@vMA41 RCCMD]#

Abb. 119: Interaktive Eingaben – Autostart, RCCMD Konfigurations-Hinweis, Installations-Abschluss

Ob die Ports wirklich offen ist, sehen Sie mit: `sudo iptables -L`

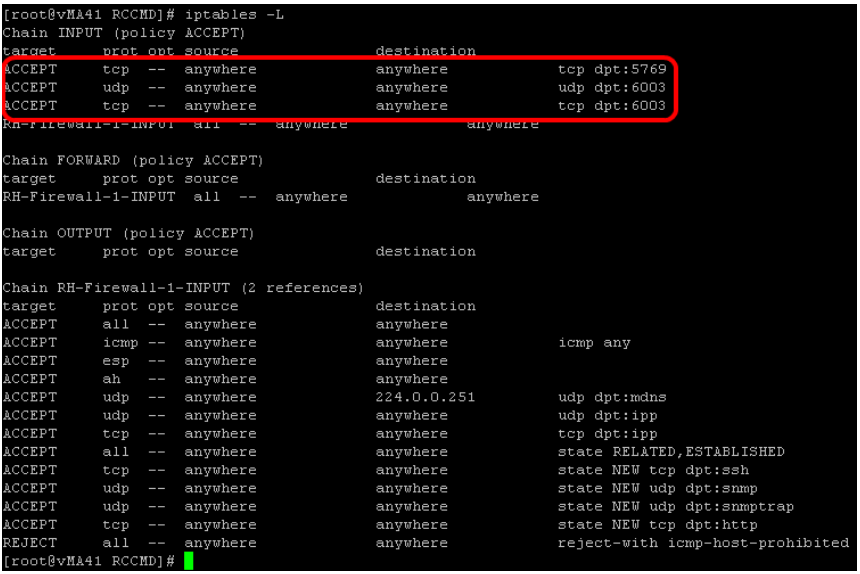

[root@vMA41 RCCMD]# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT tcp -- anywhere anywhere tcp dpt:5769
ACCEPT udp -- anywhere anywhere udp dpt:6003
ACCEPT tcp -- anywhere anywhere tcp dpt:6003
RH-Firewall-1-INPUT all -- anywhere anywhere
Chain FORWARD (policy ACCEPT)
target prot opt source destination
RH-Firewall-1-INPUT all -- anywhere anywhere
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain RH-Firewall-1-INPUT (2 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere
ACCEPT icmp -- anywhere anywhere icmp any
ACCEPT esp -- anywhere anywhere
ACCEPT ah -- anywhere anywhere
ACCEPT udp -- anywhere 224.0.0.251 udp dpt:mdns
ACCEPT udp -- anywhere anywhere udp dpt:ipp
ACCEPT tcp -- anywhere anywhere tcp dpt:ipp
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh
ACCEPT udp -- anywhere anywhere state NEW udp dpt:snmp
ACCEPT udp -- anywhere anywhere state NEW udp dpt:snmptrap
ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:http
REJECT all -- anywhere anywhere reject-with icmp-host-prohibited
[root@vMA41 RCCMD]#

Abb. 120: Auflistung IP-Tables, man sieht am „ACCEPT“ das TCP und UDP Port 6003 offen sind, weiterhin TCP Port 5769

RCCMD Konfiguration

Während der Installation wurde darauf hingewiesen, dass RCCMD ohne Einschränkung gestartet wird. Um Berechtigungen einzustellen, sehen Sie dazu in diesem Handbuch auf Seite 41, wie man die Konfigurations-Datei « rccmd.cfg » manuell editiert.

Hinweis: **Die Redundanz Funktion wird auch in der „rccmd.cfg“ manuell konfiguriert.**

Einstellungen im Shutdownscript “rccmd_shutdown.sh“

In dieser Datei wird der Shutdown dieses (und eventuell weiterer ESXi Server) eingestellt. Um die anzupassen kann z.b. ein VI Editor verwendet werden.

/usr/rccmd/rccmd_shutdown.sh angepasst werden, z. B. mit dem Aufruf:

```
vi rccmd_shutdown.sh
```

Wenn Sie mehrere ESXi Server herunterfahren möchten, ist es erforderlich die entsprechenden Zeilen hinzuzufügen, wie die Beispielzeilen in dem Kommentar der „rccmd_shutdown.sh“ im folgenden Bild.

Im Beispiel unten ist es auskommentiert, allerdings würde wenn aktiviert die .esxi_creds_HOST2 dann den 2ten, und ..HOST3 den 3ten ESXi Server herunterfahren.

```
#!/bin/sh

# rccmd_shutdown.sh - This script is called by rccmd after receiving
# the "SHUTDOWN" command from the network.

cd /                            # some systems need this!

# shutdown ESXi host

# /usr/rccmd/shutdown_ESXI.pl --config /usr/rccmd/.esxi_creds_HOST2
# /usr/rccmd/shutdown_ESXI.pl --config /usr/rccmd/.esxi_creds_HOST3

/usr/rccmd/shutdown_ESXI.pl --config /usr/rccmd/.esxi_creds
```

Abb. 121: Konfiguration rccmd_shutdown.sh, mit Beispiel für Shutdown von Host 2 und 3

Um also mehrere ESXi Server aus diesem Script herunterzufahren muss die Datei /`usr/rccmd/.esxi_creds` für jeden Host kopiert werden und dann für jeden Host um die Logindaten angepasst werden, z. B. mit dem VI Editor:

```
VI_SERVER = <Host IP>
VI_USERNAME = <Username>
VI_PASSWORD = <Password>
.esxi_creds_HOST1 (END)
```

Abb. 122: Editierung der Datei .esxi_creds

Damit die Änderungen aktiviert werden, ist es erforderlich, den RCCMD Client neuzustarten. Wechseln Sie in das Installations-Verzeichnis `/usr/rccmd /` (Standard) und geben Sie Folgendes ein:

`sudo ./rccmdctl stop` bzw. `sudo ./rccmdctl start`

Hinweis:

Es wird empfohlen, RCCMD auch auf den virtuellen Gastsystemen zu installieren und diese VOR dem physikalischen Hostrechner herunterzufahren. Dies garantiert ein sauberes Herunterfahren der virtuellen Maschinen und verhindert den möglichen Datenverlust durch ein nicht erfolgreiches Hibernating.

Hinweis:

Sie können auch eine „Silent Installation“ durchführen. Schauen Sie hierfür in das Kapitel 5.1 auf Seite 60.

11. RCCMD AS400-Client

RCCMD für AS400, eine iSeries, ist in diesem Handbuch nicht beschrieben, aber hat identische Funktionen eines jeden anderen RCCMD Systems. RCCMD für AS400 wird mit einem separaten Handbuch mit dem Produkt ausgeliefert.

Download AS400 RCCMD Benutzerhandbuch

12. RCCMD FAQ

In diesem Kapitel werden bekannte Probleme mit RCCMD behandelt bzw. Hinweise für Lösungen gegeben.

FAQ – Frequently asked Questions – Fragen & Antworten

Fehler: Die Ausführung von „sudo sh rccmd_shutdow.sh“ auf ESXi 4 mit vMA 4.1 schlägt mit der folgenden oder einer ähnlichen Fehlermeldung fehl:

„Compilation failed in require at /usr/lib/perl5/site_perl/5.8.8/VMware/VIFPLib.pm line 10 BEGIN failed.“

„Compilation aborted at /usr/lib/perl5/site_perl/5.8.8/VMware/VIFPLib.pm line 10. Compilation failed in require at /usr/rccmd/upsVIShutdown.pl line 12.“

„Can't load '/usr/lib/perl5/site_perl/5.8.8/libvmatargetlib_perl.so' for module vmatargetlib_perl: libtypes.so: cannot open shared object file: No such file or directory at /usr/lib64/perl5/5.8.8/x86_64-linux-thread-multi/DynaLoader.pm line 230.“

„BEGIN failed--compilation aborted at /usr/rccmd/upsVIShutdown.pl line 12. at /usr/lib/perl5/site_perl/5.8.8/VMware/VmaTargetLib.pm line 10.“

Ursache: Sie versuchen eine RCCMD Version für die vMA 4.0 zu installieren, welche auf vMA 4.1 oder höher zu diesem Fehler führt.

Lösung: Die RCCMD Version für die vMA 4.1 oder höher verwenden.

Problem: Shutdown von SAN/NAS Storage Systemen

Lösung: Generell benötigen die SAN/NAS Systeme, die uns bekannt sind, keinen Shutdown, wenn die Netzwerk-Computer zuvor heruntergefahren wurden. Die meisten, professionellen SAN/NAS Systeme verfügen über eine interne, gepufferte Stromversorgung, sodass genug Zeit bleibt, die Festplatten-Schreibköpfe vor dem Ausschalten an der Seite zu parken. Eine USV-Kommunikation ist nur erforderlich, wenn aus irgendeinem Grund die Netzwerk-Computer nicht heruntergefahren sind, bevor die SAN/NAS Systeme ausgeschaltet werden.

In diesem Fall besteht das Risiko, dass die zwischengespeicherten Daten im Cache der SAN/NAS Systeme verloren gehen.

Also solange RCCMD auf allen Computern ausgeführt wird, bevor die Stromversorgung abgeschaltet wird, besteht kein Risiko, Daten zu verlieren oder das SAN/NAS System zu beschädigen.

Der Grund, warum SAN/NAS System-Hersteller vor einer plötzlichen Abschaltung der Stromversorgung warnen, ist, dass sie befürchten, dass so ein Fall auftreten könnte, während das Netzwerk weiterarbeitet und viele Netzwerk-Computer verbunden sind. Das wäre ein wirkliches Problem, aber dies ist exakt das, was eine USV verhindern sollte!

Problem: Sie erhalten folgende Fehlermeldung bei der Ausführung der upsVIShutdown.pl:

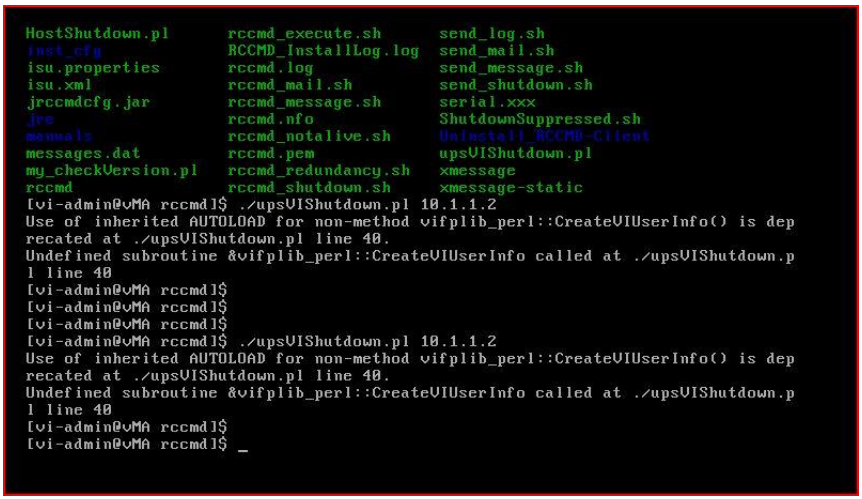


Abb. 123: Fehlermeldung nach Ausführung der upsVIShutdown.pl

Lösung: Sie verwenden nicht die aktuellste RCCMD Version. Bitte laden Sie das neueste Download-Paket von unserer Webseite www.generex.de herunter.

Problem: Shutdown von NetApp Storages

Lösung: Generell exportieren alle NAS Systeme Ihre NFS Shares im "Async" Modus. Dies ist ein extrem schneller Schreibprozess, der gewährleistet, dass bei einem plötzlichen Stromausfall kein Datenverlust entsteht. Solange der Anwender den Standard NFS Protokoll Schreibmodus von "Async" auf "Sync" verändert hat, besteht kein Risiko, Daten zu verlieren. QNAP Systeme mit "Sync" Modus besitzen eine eigene Batterie, um einen sicheren Shutdown gewährleisten zu können und manchmal auch Shutdown-Tools mit Strom zu versorgen, die von jedem LAN PC ausgeführt werden können. In solchem Fall ist RCCMD ideal, wenn bereits auf einem anderen PC installiert.

Nutzen Sie einen Editor, öffnen Sie das Shutdown-Script (shutdown.bat oder rccmd_shutdown_sh), und tragen Sie den NAS Shutdown-Befehl

```
halt [-d halt_string] [-f] [-t interval]
```

VOR dem Shutdown des RCCMD Clients ein!

Problem: Fehlermeldungen bei „UPSMAN Alive Check“ auf Windws Server 2008

Lösung: Der Firewall Port 5769 muss für alle Profile (Domäne, Heim, öffentlich) freigeschaltet werden!

Appendix

A OpenSSL

"This product includes software developed by the OpenSSL Project for use

in the OpenSSL Toolkit (http://www.openssl.org/).

B Syntax zum Schalten von Ausgängen

Den RCCMD Empfänger auf Port 6002 auf „On“ stellen, die AUX-Ports des CS121 als Outputs definieren und neu starten. Installieren Sie den RCCMD Windows Wizard, und öffnen Sie eine DOS-Box. Es folgt ein Syntax-Beispiel mit der IP-Adresse 192.168.202.165:

```
C:\Program Files\RCCMD\
```

```
rccmd -se "EXECUTE |AUX|1|1" -s -a 192.168.202.165 -p 6002
```

ACHTUNG! Die Leerzeile nach dem EXECUTE ist wichtig!

Allgemeine Syntax für das Schalten von AUX Ports:

```
|AUX|1|0  Port1, auf low setzen
|AUX|1|1  Port1, auf high setzen
|AUX|2|0  Port2, auf low setzen
|AUX|2|1  Port2, auf high setzen
|AUX|3|0  Port3, auf low setzen
|AUX|3|1  Port3, auf high setzen
|AUX|4|0  Port4, auf low setzen
|AUX|4|1  Port4, auf high setzen
```

Syntax-Beispiel für das Schalten der Outputs am SiteManager:

```
C:\Program Files\RCCMD\rccmd -s -a 192.168.222.238 -p 6002 -se
"EXECUTE |UPSCMD|20000|1,1"
```

ACHTUNG! Die Leerzeile nach dem EXECUTE ist wichtig!

```
|UPSCMD|20000|1,0  Ausgang 1 auf low
|UPSCMD|20000|1,1  Ausgang 1 auf high
|UPSCMD|20000|2,0  Ausgang 2 auf low
|UPSCMD|20000|2,1  Ausgang 2 auf high
|UPSCMD|20000|3,0  Ausgang 3 auf low
|UPSCMD|20000|3,1  Ausgang 3 auf high
|UPSCMD|20000|4,0  Ausgang 4 auf low
|UPSCMD|20000|4,1  Ausgang 4 auf high
|UPSCMD|20000|5,0  Ausgang 5 auf low
|UPSCMD|20000|5,1  Ausgang 5 auf high
|UPSCMD|20000|6,0  Ausgang 6 auf low
|UPSCMD|20000|6,1  Ausgang 6 auf high
|UPSCMD|20000|7,0  Ausgang 7 auf low
|UPSCMD|20000|7,1  Ausgang 7 auf high
|UPSCMD|20000|8,0  Ausgang 8 auf low
|UPSCMD|20000|8,1  Ausgang 8 auf high
```

C Know How Pool

SuSE 8.1 und ältere Linux Versionen

Wenn Sie SuSE 8.1 oder eine ältere Linux Version nutzen, müssen Sie während der interaktiven RCCMD Installation als OS „XEN-Server“ auswählen!

D Abbildungen

Abb. 1: RCCMD und UPSMAN in einer Netzwerkumgebung 6

Abb. 2: Einführung 7

Abb. 3: Lizenzschlüssel Eintrag 8

Abb. 4: Lizenzvertrag 8

Abb. 5: Auswahl Installationsordner 9

Abb. 6: Auswahl Verknüpfungsordner 10

Abb. 7: Preinstallations Übersicht 10

Abb. 8: Client Installation 11

Abb. 9: Eingabe IP-Adresse 11

Abb. 10: Erweiterte Netzwerk Einstellungen 12

Abb. 11: UPSMAN Alive Checking / Redundanz Fenster 13

Abb. 12: Client Check Connection Batch File Fenster 14

Abb. 13: Check UPSMAN Connections Fenster 15
Abb. 14: Konfiguration der Batch Files Fenster 15
Abb. 15: RCCMD Log File 16
Abb. 16: RCCMD Shutdown Sequenz Konfiguration 16
Abb. 17: Dateiinhalt „installer.properties“ 18
Abb. 18: Erfolgreiches Client Installations Fenster 20
Abb. 19: Lizenzschlüssel Eintrag 22
Abb. 20: RCCMD Setup Typ Fenster 23
Abb. 21: Eingabe Lizenzschlüssel 23
Abb. 22: RCCMD Eigenschaften Fenster 24
Abb. 23: RCCMD Eigenschaften Log On Fenster 25
Abb. 24: RCCMD Eigenschaften Passwort-Bestätigung 25
Abb. 25: Select User Fenster 26
Abb. 26: Auswahl des Objektnamens 26
Abb. 27: Administrator Auswahl 27
Abb. 28: Administrator Passwort Bestätigung 27
Abb. 29: Dienst-Berechtigungs-Fenster 28
Abb. 30: Client Installation RCCMD Redundanz 28
Abb. 31: Client Installation RCCMD Redundanz Konfiguration 29
Abb. 32: CS121 Konfiguration „WAKEUP“ Befehl 30
Abb. 33: UPSMAN Konfiguration „WAKEUP“ Befehl 31
Abb. 34: „WAKEUP“ Befehl im RCCMD Log 31
Abb. 35: Example: Batch File RCCMD als Relay Station 32
Abb. 36: RCCMD Client Shutdown Konfiguration 33
Abb. 37: RCCMD Shutdown Relay 33
Abb. 38: RCCMD Konfiguration IP-Adressen-Bereich 34
Abb. 39: RCCMD Shutdown Relay Adress-Entfernung 34
Abb. 40: RCCMD Shutdown Relay in der „Shutdwown.bat“ 35
Abb. 41: RCCMD Konfiguration 38

Abb. 42: RCCMD SSL Einstellung 39
Abb. 43: Timeserver Konfiguration 39
Abb. 44: Speichern der Einstellungen 40
Abb. 45: SSL Konfiguration 40
Abb. 46: Advanced Network Settings 41
Abb. 47: RCCMD Konsolen-Test 46
Abb. 48: RCCMD Alive Check via Befehlszeile 47
Abb. 49: UPSMAN Alive Check Fenster 47
Abb. 50: RCCMD Konsole -? 48
Abb. 51: Installation – Einführung 53
Abb. 52: Installation – Lizenzeingabe 53
Abb. 53: Installation – Ordnerauswahl 54
Abb. 54: Installation – Auswahl der Wiedergabemöglichkeiten 54
Abb. 55: Installation – Prä-Installations-Übersicht 55
Abb. 56: Konfiguration – IP-Adressen Fenster 55
Abb. 57: Konfiguration – Functions 56
Abb. 58: Konfiguration – RCCMD Redundanz 57
Abb. 59: Konfiguration – RCCMD Log File 58
Abb. 60: Konfiguration – RCCMD Execute 58
Abb. 61: Konfiguration – RCCMD Configure Email 59
Abb. 62: Konfiguration – RCCMD Shutdown.sh 59
Abb. 63: Konfiguration – RCCMD Shutdown Sequenz 60
Abb. 64: Konfiguration – RCCMD Control 61
Abb. 65: Konfiguration – RCCMD mit Redundanz 62
Abb. 66: Dateiinhalt „installer.properties“ 63
Abb. 67: Erstellung des Konfigurations-Files 67
Abb. 68: RCCMD Konfigurations-Menü UNIX 68
Abb. 69: RCCMD UNIX Netzwerk Optionen 69
Abb. 70: Hinzufügen RCCMD UNIX Sender 71

Abb. 71: RCCMD UNIX Sender Beispiel 71
Abb. 72: RCCMD UNIX Sender Überblick 72
Abb. 73: RCCMD UNIX Sender Editierung 72
Abb. 74: RCCMD UNIX Sender Löschen 73
Abb. 75: RCCMD UNIX Sender Scan 74
Abb. 76: RCCMD UNIX Check Upsman 75
Abb. 77: RCCMD UNIX Log File Optionen 76
Abb. 78: RCCMD UNIX Shutdown Optionen 77
Abb. 79: RCCMD UNIX File Browsing 78
Abb. 80: Konfiguration – RCCMD Shutdown.sh 81
Abb. 81: Konfiguration – RCCMD Shutdown Sequenz 81
Abb. 82: Konfiguration – RCCMD Relay Konfiguration IP-Adressen-Bereich 82
Abb. 83: RCCMD SSL Konfiguration 82
Abb. 84: Timeserver Konfiguration 83
Abb. 88: Mac OS RCCMD Installations-Start 90
Abb. 89: Mac OS RCCMD Konfiguration 90
Abb. 90: Mac OS hinzufügen/modifizieren gültiger Remote Stations 91
Abb. 91: Mac OS Lizenz Schlüssel Eintrag 91
Abb. 92: Mac OS Verzögerungs-Option 92
Abb. 93: Mac OS Aktuelle Einstellungen 92
Abb. 94: Mac OS hinzufügen von RCCMD Empfängern (RCCMD Clients) 93
Abb. 95: RCCMD Installations-Willkommen 94
Abb. 96: RCCMD Lizenz Schlüssel Eingabe 94
Abb. 97: Prä-Installations-Übersicht 95
Abb. 98: RCCMD IP Adressen Fenster 95
Abb. 99: RCCMD Konfigurations-Fenster „Functions“ 96
Abb. 100: RCCMD Check UPSMAN Verbindungen 97
Abb. 101: RCCMD Redundanz 97
Abb. 102: RCCMD Konfigurations-Fenster „Logfile“ 98

Abb. 103: RCCMD Konfigurations-Fenster „Execute“ 98
Abb. 104: RCCMD E-Mail-Konfiguration 99
Abb. 105: Konfiguration – RCCMD Shutdown.sh 99
Abb. 106: Konfiguration – RCCMD Shutdown Sequenz 100
Abb. 107: RCCMD Control 101
Abb. 108: Firewall Konfiguration 102
Abb. 109: VMware Products 103
Abb. 110: ESXi Lizenz-Fehlermeldung bei kostenloser ESXi Lizenz 106
Abb. 111: vSphere-Client Konfiguration 107
Abb. 112: vSphere-Client Autostart-Konfiguration 108
Abb. 113: vSphere-Client Autostart-Verzögerung 108
Abb. 114: Installationsvorbereitung 109
Abb. 115: Ausführung der Binärdatei 109
Abb. 116: Sprachauswahl 110
Abb. 117: Interaktive Eingaben – ESXi Userdetails, Kennwort 111
Abb. 118: Installer meldet das Firewall Port 6003 und 5769 geöffnet wurden 111
Abb. 119: Interaktive Eingaben – Autostart, RCCMD Konfigurations-Hinweis, Installations-Abschluss 112
Abb. 120: Auflistung IP-Tables, man sieht am „ACCEPT“ das TCP und UDP Port 6003 offen sind, weiterhin TCP Port 5769 113
Abb. 121: Konfiguration rccmd_shutdown.sh, mit Beispiel für Shutdown von Host 2 114
Abb. 122: Editierung der Datei .esxi_creds 114
Abb. 123: Fehlermeldung nach Ausführung der upsVIShutdown.pl 116